The Structure of Risk Management in Leading Australian Companies

Research submitted for the award of Doctor of Business Administration
Charles Sturt University
Steven W Halliday, BCom, MBA, MLaw
October 2013
<table>
<thead>
<tr>
<th>Section</th>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Table of Contents</td>
<td>i</td>
</tr>
<tr>
<td></td>
<td>Table of Figures</td>
<td>vii</td>
</tr>
<tr>
<td></td>
<td>List of Abbreviations</td>
<td>xi</td>
</tr>
<tr>
<td></td>
<td>Certificate of Authorship</td>
<td>xiv</td>
</tr>
<tr>
<td></td>
<td>About the Author</td>
<td>xv</td>
</tr>
<tr>
<td></td>
<td>Acknowledgements</td>
<td>xvi</td>
</tr>
<tr>
<td></td>
<td>Abstract</td>
<td>xviii</td>
</tr>
<tr>
<td></td>
<td><strong>Chapter One - Introduction</strong></td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>1.2</td>
<td>The Need for the Research</td>
<td>4</td>
</tr>
<tr>
<td>1.3</td>
<td>Developing the Research Objectives</td>
<td>8</td>
</tr>
<tr>
<td>1.4</td>
<td>Research Methodology</td>
<td>9</td>
</tr>
<tr>
<td>1.5</td>
<td>Findings</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td><strong>Chapter Two – Literature Review</strong></td>
<td></td>
</tr>
<tr>
<td>2.1</td>
<td>Introduction</td>
<td>15</td>
</tr>
<tr>
<td>2.2</td>
<td>Overview of this Chapter</td>
<td>15</td>
</tr>
<tr>
<td>2.3</td>
<td>Theoretical Frameworks</td>
<td>18</td>
</tr>
<tr>
<td>2.3.1</td>
<td>Agency Theory</td>
<td>20</td>
</tr>
<tr>
<td>2.3.2</td>
<td>Institutional Theory</td>
<td>25</td>
</tr>
<tr>
<td>2.3.3</td>
<td>Contingency Theory</td>
<td>31</td>
</tr>
<tr>
<td>2.3.4</td>
<td>Signalling Theory</td>
<td>34</td>
</tr>
<tr>
<td>2.3.5</td>
<td>Knowledge Management</td>
<td>37</td>
</tr>
<tr>
<td>2.3.6</td>
<td>Power Theory</td>
<td>45</td>
</tr>
<tr>
<td>2.3.7</td>
<td>Life-Cycle Model</td>
<td>48</td>
</tr>
<tr>
<td>2.4</td>
<td>The Definition of Governance</td>
<td>50</td>
</tr>
<tr>
<td>2.5</td>
<td>The Liability of Company Directors</td>
<td>56</td>
</tr>
<tr>
<td>2.6</td>
<td>Board Audit or Risk Committees</td>
<td>60</td>
</tr>
<tr>
<td>2.6.1</td>
<td>Board Audit Committee</td>
<td>61</td>
</tr>
<tr>
<td>2.6.2</td>
<td>Board Risk Committee</td>
<td>66</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>2.7</td>
<td>Skill, Timing and Workload Issues</td>
<td>73</td>
</tr>
<tr>
<td>2.8</td>
<td>Adoption of ERM</td>
<td>76</td>
</tr>
<tr>
<td>2.9</td>
<td>Executive Governance over Risk Management</td>
<td>84</td>
</tr>
<tr>
<td>2.10</td>
<td>The Integration of Audit and Risk</td>
<td>90</td>
</tr>
<tr>
<td>2.10.1</td>
<td>The Oversight of Internal Audit and Links to Risk Management</td>
<td>91</td>
</tr>
<tr>
<td>2.10.2</td>
<td>An Emerging Paradigm Shift</td>
<td>95</td>
</tr>
<tr>
<td>2.11</td>
<td>The Synergies between Audit and Risk</td>
<td>100</td>
</tr>
<tr>
<td>2.11.1</td>
<td>Management Responsibility</td>
<td>102</td>
</tr>
<tr>
<td>2.11.2</td>
<td>Functional Objectives</td>
<td>103</td>
</tr>
<tr>
<td>2.11.3</td>
<td>Systems of Internal Control</td>
<td>104</td>
</tr>
<tr>
<td>2.11.4</td>
<td>Three Lines of Defence</td>
<td>105</td>
</tr>
<tr>
<td>2.11.5</td>
<td>Efficiency and Effectiveness</td>
<td>106</td>
</tr>
<tr>
<td>2.12</td>
<td>Barriers to Integration</td>
<td>107</td>
</tr>
<tr>
<td>2.12.1</td>
<td>Auditor Independence</td>
<td>107</td>
</tr>
<tr>
<td>2.12.2</td>
<td>Is Auditor Independence an Illusion?</td>
<td>110</td>
</tr>
<tr>
<td>2.12.3</td>
<td>The Role for Internal Audit in Risk Management</td>
<td>117</td>
</tr>
<tr>
<td>2.13</td>
<td>Evidence of Integration</td>
<td>120</td>
</tr>
<tr>
<td>2.13.1</td>
<td>United States and Canada</td>
<td>121</td>
</tr>
<tr>
<td>2.13.2</td>
<td>United Kingdom</td>
<td>122</td>
</tr>
<tr>
<td>2.13.3</td>
<td>Australia</td>
<td>123</td>
</tr>
<tr>
<td>2.14</td>
<td>Outsourcing versus Co-sourcing</td>
<td>125</td>
</tr>
<tr>
<td>2.15</td>
<td>Research Objectives</td>
<td>128</td>
</tr>
<tr>
<td>2.15.1</td>
<td>Research Objective One – Structural Arrangements</td>
<td>129</td>
</tr>
<tr>
<td>2.15.2</td>
<td>Research Objective Two – Levels of Integration</td>
<td>132</td>
</tr>
<tr>
<td>2.15.3</td>
<td>Research Objective Three – Models for Risk Management</td>
<td>135</td>
</tr>
</tbody>
</table>

**Chapter Three – Research Methodology**

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>Introduction</td>
<td>139</td>
</tr>
<tr>
<td>3.2</td>
<td>Research Questions</td>
<td>140</td>
</tr>
<tr>
<td>3.3</td>
<td>Overview of Methodology</td>
<td>141</td>
</tr>
<tr>
<td>3.4</td>
<td>The S&amp;P/ASX 200 Companies</td>
<td>145</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>3.5</td>
<td>Stage 1 – Desk Top Analysis</td>
<td>147</td>
</tr>
<tr>
<td>3.6</td>
<td>Stage 2 - Survey</td>
<td>152</td>
</tr>
<tr>
<td>3.6.1</td>
<td>Population and Sample Selection</td>
<td>152</td>
</tr>
<tr>
<td>3.6.2</td>
<td>Data Collection</td>
<td>153</td>
</tr>
<tr>
<td>3.6.3</td>
<td>Design of the Survey Questions</td>
<td>154</td>
</tr>
<tr>
<td>3.6.4</td>
<td>Design of the Survey Format</td>
<td>155</td>
</tr>
<tr>
<td>3.6.5</td>
<td>Validation of the Survey</td>
<td>155</td>
</tr>
<tr>
<td>3.7</td>
<td>Stage 3 - Interviews</td>
<td>163</td>
</tr>
<tr>
<td>3.7.1</td>
<td>The Need for Interviews</td>
<td>163</td>
</tr>
<tr>
<td>3.7.2</td>
<td>Interview Techniques</td>
<td>164</td>
</tr>
<tr>
<td>3.7.3</td>
<td>Chosen Technique</td>
<td>164</td>
</tr>
<tr>
<td>3.7.4</td>
<td>Problems with Interview Techniques</td>
<td>165</td>
</tr>
<tr>
<td>3.7.5</td>
<td>Interview Questions</td>
<td>169</td>
</tr>
<tr>
<td>3.7.6</td>
<td>Interview Process</td>
<td>172</td>
</tr>
<tr>
<td>3.8</td>
<td>Data Analysis</td>
<td>178</td>
</tr>
<tr>
<td>3.8.1</td>
<td>Cleaning the Data-sets</td>
<td>178</td>
</tr>
<tr>
<td>3.8.2</td>
<td>Examining the Data-sets</td>
<td>179</td>
</tr>
<tr>
<td>3.8.3</td>
<td>Data Relationships</td>
<td>181</td>
</tr>
<tr>
<td>3.8.3</td>
<td>Graphical and Descriptive Analysis</td>
<td>184</td>
</tr>
<tr>
<td>3.8.4</td>
<td>Analysing the Interviews</td>
<td>184</td>
</tr>
<tr>
<td>3.9</td>
<td>Research Validation</td>
<td>191</td>
</tr>
<tr>
<td></td>
<td><strong>Chapter Four - Findings</strong></td>
<td></td>
</tr>
<tr>
<td>4.1</td>
<td>Introduction</td>
<td>197</td>
</tr>
<tr>
<td>4.2</td>
<td>At Board Committee Level</td>
<td>198</td>
</tr>
<tr>
<td>4.3</td>
<td>Board Audit and Risk Committees</td>
<td>202</td>
</tr>
<tr>
<td>4.4</td>
<td>The Synergies between Internal Audit and Risk Management</td>
<td>204</td>
</tr>
<tr>
<td>4.4.1</td>
<td>Circular Flow</td>
<td>205</td>
</tr>
<tr>
<td>4.4.2</td>
<td>Three Lines of Defence</td>
<td>212</td>
</tr>
<tr>
<td>4.4.3</td>
<td>Accounts are the Culmination of Risk Management</td>
<td>214</td>
</tr>
<tr>
<td>4.4.4</td>
<td>Similarity between Internal Audit and Risk Management</td>
<td>218</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>4.4.5</td>
<td>Alignment with Compliance</td>
<td>220</td>
</tr>
<tr>
<td>4.5</td>
<td>Separate Board Risk Committees</td>
<td>221</td>
</tr>
<tr>
<td>4.5.1</td>
<td>The Financial Services Sector (GICS 40)</td>
<td>223</td>
</tr>
<tr>
<td>4.5.2</td>
<td>The Consumer Products Sector (GICS 25 &amp; 30)</td>
<td>229</td>
</tr>
<tr>
<td>4.5.3</td>
<td>Three Sectors without Board Risk Committees</td>
<td>232</td>
</tr>
<tr>
<td>4.6</td>
<td>No Board Risk Committee</td>
<td>236</td>
</tr>
<tr>
<td>4.7</td>
<td>Skill, Timing and Workload Issues</td>
<td>238</td>
</tr>
<tr>
<td>4.8</td>
<td>Enterprise Risk Management (ERM)</td>
<td>243</td>
</tr>
<tr>
<td>4.9</td>
<td>Executive Management Oversight of Risk</td>
<td>248</td>
</tr>
<tr>
<td>4.10</td>
<td>Integration at the Functional Level</td>
<td>254</td>
</tr>
<tr>
<td>4.10.1</td>
<td>Reasons for Integration between Internal Audit and Risk Management</td>
<td>259</td>
</tr>
<tr>
<td>4.10.2</td>
<td>Integration and Independence</td>
<td>261</td>
</tr>
<tr>
<td>4.10.3</td>
<td>Separated Functional Teams</td>
<td>262</td>
</tr>
<tr>
<td>4.11</td>
<td>Outsourcing of Internal Audit</td>
<td>265</td>
</tr>
<tr>
<td>4.12</td>
<td>No Internal Audit</td>
<td>271</td>
</tr>
<tr>
<td>4.12.1</td>
<td>Revenues</td>
<td>272</td>
</tr>
<tr>
<td>4.12.2</td>
<td>Industry Classification</td>
<td>272</td>
</tr>
<tr>
<td>4.12.3</td>
<td>Interviews with No Internal Audit Companies</td>
<td>273</td>
</tr>
<tr>
<td>4.13</td>
<td>Interviews with Executives</td>
<td>276</td>
</tr>
<tr>
<td>4.13.1</td>
<td>Integration of Audit and Risk</td>
<td>279</td>
</tr>
<tr>
<td>4.13.2</td>
<td>Synergy Between Audit and Risk</td>
<td>279</td>
</tr>
<tr>
<td>4.13.3</td>
<td>The Independence Barrier</td>
<td>283</td>
</tr>
<tr>
<td>4.13.4</td>
<td>Combined Roles</td>
<td>287</td>
</tr>
<tr>
<td>4.13.5</td>
<td>Organisational Maturity</td>
<td>289</td>
</tr>
<tr>
<td>4.13.6</td>
<td>Prior Development and Experience</td>
<td>292</td>
</tr>
<tr>
<td>4.13.7</td>
<td>Alignment of Audit and Risk</td>
<td>294</td>
</tr>
<tr>
<td>4.13.8</td>
<td>Audit is a Subset of Risk Management</td>
<td>295</td>
</tr>
<tr>
<td>4.13.9</td>
<td>Audit as Part of the Governance Framework</td>
<td>296</td>
</tr>
<tr>
<td>4.14</td>
<td>Models for Managing Risk in Australia</td>
<td>300</td>
</tr>
<tr>
<td>4.14.1</td>
<td>Traditional Independence Model</td>
<td>303</td>
</tr>
<tr>
<td>4.14.2</td>
<td>Current Merged Model</td>
<td>306</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
<td></td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
<td></td>
</tr>
<tr>
<td>4.14.3 Emerging Model</td>
<td>309</td>
<td></td>
</tr>
<tr>
<td>4.14.4 No Internal Audit Model</td>
<td>312</td>
<td></td>
</tr>
<tr>
<td><strong>Chapter Five – Conclusion</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.1 Introduction</td>
<td>317</td>
<td></td>
</tr>
<tr>
<td>5.2 Combined Board Audit and Risk Committees</td>
<td>317</td>
<td></td>
</tr>
<tr>
<td>5.3 Separate Board Risk Committees</td>
<td>321</td>
<td></td>
</tr>
<tr>
<td>5.4 No Board Risk Committee</td>
<td>322</td>
<td></td>
</tr>
<tr>
<td>5.5 Skill and Timing Issues</td>
<td>323</td>
<td></td>
</tr>
<tr>
<td>5.6 Enterprise Risk Management</td>
<td>324</td>
<td></td>
</tr>
<tr>
<td>5.7 Executive Oversight for Risk Management</td>
<td>326</td>
<td></td>
</tr>
<tr>
<td>5.8 Integration at the Functional Level</td>
<td>328</td>
<td></td>
</tr>
<tr>
<td>5.9 Outsourcing of Internal Audit</td>
<td>330</td>
<td></td>
</tr>
<tr>
<td>5.10 Models for Managing Risk</td>
<td>331</td>
<td></td>
</tr>
<tr>
<td>5.11 Limitations of the Research</td>
<td>333</td>
<td></td>
</tr>
<tr>
<td>5.12 Contributions from the Research</td>
<td>335</td>
<td></td>
</tr>
<tr>
<td>5.13 Conclusion</td>
<td>344</td>
<td></td>
</tr>
<tr>
<td><strong>Bibliography</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Appendix One – S&amp;P/ASX 200 companies at 30 June 2007</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Appendix Two – Desk-top analysis data-set</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Appendix Three – Survey instrument</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Appendix Four – Survey analysis data-set</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Appendix Five – Table linking research objectives to survey design</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Appendix Six – Author’s article in Risk Management Magazine</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Appendix Seven – Survey Pre-notification Letter</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Appendix Eight – Information statement accompanying survey</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Appendix Nine – Survey reminder letter</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Appendix Ten – Frequency Tables for Survey Data-set Analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Appendix Eleven – Interpretive sub-codes for descriptive code “Audit and Risk Synergy”</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Appendix Twelve – Draft Abstract sent to S&amp;P/ASX 200 Executives for Discussion and Verification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Appendix Thirteen – Example Organisational Chart</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Appendix Fourteen – Key Writers on Risk Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Appendix Fifteen – Ethics approval letter</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Appendix Sixteen – Comments on survey by Tony Hocking from EMRS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Appendix Seventeen – Lawrence &amp; Lorsch (1967)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Appendix Eighteen – The Difficulty Implementing ERM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Appendix Nineteen – Survey Design Principles</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Appendix Twenty – Table Linking Findings with Theory, the Literature and Practice</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Appendix Twenty One – Rationale behind each survey question</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Figure</td>
<td>Chapter One - Introduction</td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>---------------------------</td>
<td></td>
</tr>
<tr>
<td>2.1</td>
<td>Characteristics of different stages in the company life cycle. Adapted from Dibrell et al (2011)</td>
<td>48</td>
</tr>
<tr>
<td>2.2</td>
<td>The structure of corporate governance</td>
<td>51</td>
</tr>
<tr>
<td>2.3</td>
<td>Evolution of risk management</td>
<td>78</td>
</tr>
<tr>
<td>2.4</td>
<td>Changing the paradigm</td>
<td>96</td>
</tr>
<tr>
<td>2.5</td>
<td>Old versus new internal audit paradigms</td>
<td>97</td>
</tr>
<tr>
<td>2.6</td>
<td>The next paradigm shift</td>
<td>99</td>
</tr>
<tr>
<td>2.7</td>
<td>Internal audit and ERM</td>
<td>109</td>
</tr>
<tr>
<td>2.8</td>
<td>Percentage of companies with internal audit and percentage outsourced</td>
<td>128</td>
</tr>
<tr>
<td>2.9</td>
<td>Models for the governance of risk management</td>
<td>136</td>
</tr>
<tr>
<td></td>
<td><strong>Chapter Two – Developing the Research Objectives</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Chapter Three – Research Methodology</strong></td>
<td></td>
</tr>
<tr>
<td>3.1</td>
<td>Classification of variables – desk-top analysis</td>
<td>148</td>
</tr>
<tr>
<td>3.2</td>
<td>Controlling non-response bias</td>
<td>160</td>
</tr>
<tr>
<td>3.3</td>
<td>Classification of variables – survey analysis</td>
<td>162</td>
</tr>
<tr>
<td>3.4</td>
<td>Thirty five executives interviewed in the first round of interviews during October and November 2008</td>
<td>174</td>
</tr>
<tr>
<td>3.5</td>
<td>Interview themes from first round interviews conducted over October and November 2008</td>
<td>175</td>
</tr>
<tr>
<td>3.6</td>
<td>First, second and third round interviews with executives from the S&amp;P/ASX 200 and Big Four</td>
<td>177</td>
</tr>
<tr>
<td>Section</td>
<td>Description</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td>3.7</td>
<td>Descriptive information for revenue in the S&amp;P/ASX 200 in the desk-top analysis</td>
<td>179</td>
</tr>
<tr>
<td>3.8</td>
<td>Descriptive information by GICS for the S&amp;P/ASX 200 in the desk-top analysis</td>
<td>180</td>
</tr>
<tr>
<td>3.9</td>
<td>Descriptive information on ADR for the S&amp;P/ASX 200 in the desk-top analysis</td>
<td>180</td>
</tr>
<tr>
<td>3.10</td>
<td>REV (Revenue in A$ million) and YRS (Years since incorporation) for S&amp;P/ASX 200 companies from the survey analysis</td>
<td>181</td>
</tr>
<tr>
<td>3.11</td>
<td>Categories of variables for desk-top analysis data-set</td>
<td>182</td>
</tr>
<tr>
<td>3.12</td>
<td>Categories of variables for survey analysis data-set</td>
<td>183</td>
</tr>
<tr>
<td>3.13</td>
<td>Descriptive coding from interviews with thirty five S&amp;P/ASX 200 executives</td>
<td>188</td>
</tr>
<tr>
<td>3.14</td>
<td>Interpretive coding for interview question on audit and risk synergy</td>
<td>189</td>
</tr>
<tr>
<td>3.15</td>
<td>Table of research validation comments from S&amp;P/ASX 200 executives</td>
<td>196</td>
</tr>
</tbody>
</table>

**Chapter Four – Findings**

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>Board risk committee arrangements in the S&amp;P/ASX 200 companies</td>
<td>199</td>
</tr>
<tr>
<td>4.2</td>
<td>Triangulation of desk-top analysis results with survey results</td>
<td>200</td>
</tr>
<tr>
<td>4.3</td>
<td>Chi Square for figure 4.2</td>
<td>200</td>
</tr>
<tr>
<td>4.4</td>
<td>Reasons for combining board audit and risk committees</td>
<td>203</td>
</tr>
<tr>
<td>4.5</td>
<td>The internal audit and risk management “Circular Flow”</td>
<td>207</td>
</tr>
<tr>
<td>4.6</td>
<td>Risk management underpins the annual accounts (the “Iceberg” model)</td>
<td>215</td>
</tr>
<tr>
<td>4.7</td>
<td>Separate board risk committee by GICS</td>
<td>222</td>
</tr>
<tr>
<td>Section</td>
<td>Description</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>4.8</td>
<td>Reasons for separate board committee GICS 40 financial services companies</td>
<td>223</td>
</tr>
<tr>
<td>4.9</td>
<td>Reasons for adopting a separate board risk committee in GICS 25 &amp; 30 sectors</td>
<td>230</td>
</tr>
<tr>
<td>4.10</td>
<td>Skill, timing and workload issues with combined board audit and risk committees</td>
<td>239</td>
</tr>
<tr>
<td>4.11</td>
<td>State of ERM development in S&amp;P/ASX 200 companies</td>
<td>244</td>
</tr>
<tr>
<td>4.12</td>
<td>Adoption of ERM by S&amp;P/ASX 200 companies</td>
<td>245</td>
</tr>
<tr>
<td>4.13</td>
<td>Average revenue for S&amp;P/ASX 200 companies by Likert category</td>
<td>246</td>
</tr>
<tr>
<td>4.14</td>
<td>Average Likert score for S&amp;P/ASX 200 companies by GICS</td>
<td>247</td>
</tr>
<tr>
<td>4.15</td>
<td>Executive oversight of risk management in S&amp;P/ASX 200 companies</td>
<td>249</td>
</tr>
<tr>
<td>4.16</td>
<td>Executive management oversight of risk in the S&amp;P/ASX 200 by GICS</td>
<td>250</td>
</tr>
<tr>
<td>4.17</td>
<td>Chi Square for figure 4.16</td>
<td>251</td>
</tr>
<tr>
<td>4.18</td>
<td>Separation of internal audit and risk management at the functional level in the S&amp;P/ASX 200 companies</td>
<td>255</td>
</tr>
<tr>
<td>4.19</td>
<td>Comparison of survey responses to interview responses in the S&amp;P/ASX 200 companies</td>
<td>257</td>
</tr>
<tr>
<td>4.20</td>
<td>Reasons for integrating audit and risk in the S&amp;P/ASX 200 companies</td>
<td>259</td>
</tr>
<tr>
<td>4.21</td>
<td>Independence concerns for integrated risk and audit teams in the S&amp;P/ASX 200 companies</td>
<td>261</td>
</tr>
<tr>
<td>4.22</td>
<td>Reasons for separating internal audit from risk management in the S&amp;P/ASX 200 companies</td>
<td>263</td>
</tr>
<tr>
<td>4.23</td>
<td>Levels of co-sourcing and outsourcing in the S&amp;P/ASX 200 companies</td>
<td>266</td>
</tr>
<tr>
<td>Section</td>
<td>4.24 Internal audit and outsourcing comparisons</td>
<td>4.25 Average revenue for outsourced and co-sourced internal audit in the S&amp;P/ASX 200 companies</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------------------------</td>
</tr>
<tr>
<td>Page</td>
<td>267</td>
<td>270</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Definition</td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
<td></td>
</tr>
<tr>
<td>ACI</td>
<td>Australian Compliance Institute</td>
<td></td>
</tr>
<tr>
<td>ADR</td>
<td>Audit and Risk arrangement at Board Level</td>
<td></td>
</tr>
<tr>
<td>AFAANZ</td>
<td>Accounting and Finance Association of Australia and New Zealand</td>
<td></td>
</tr>
<tr>
<td>AFSL</td>
<td>Australian Financial Services Licence</td>
<td></td>
</tr>
<tr>
<td>AICPA</td>
<td>American Institute of Certified Public Accountants</td>
<td></td>
</tr>
<tr>
<td>APRA</td>
<td>Australian Prudential Regulatory Authority</td>
<td></td>
</tr>
<tr>
<td>ASIC</td>
<td>Australian Securities and Investment Commission</td>
<td></td>
</tr>
<tr>
<td>ASX</td>
<td>Australian Securities Exchange</td>
<td></td>
</tr>
<tr>
<td>ASX Principles</td>
<td>Australian Securities Exchange, Principles of Good Corporate Governance and Best Practice Recommendations</td>
<td></td>
</tr>
<tr>
<td>Big Four</td>
<td>The four largest international accounting, auditing and consulting firms: Ernst &amp; Young, Deloitte, KPMG and PricewaterhouseCoopers</td>
<td></td>
</tr>
<tr>
<td>CAE</td>
<td>Chief Audit Executive</td>
<td></td>
</tr>
<tr>
<td>CAMAC</td>
<td>Corporations and Markets Advisory Committee</td>
<td></td>
</tr>
<tr>
<td>CCO</td>
<td>Chief Compliance Officer</td>
<td></td>
</tr>
<tr>
<td>CEO</td>
<td>Chief Executive Officer</td>
<td></td>
</tr>
<tr>
<td>CFO</td>
<td>Chief Financial Officer</td>
<td></td>
</tr>
<tr>
<td>CLERP</td>
<td>Corporate Law Economic Reform Program</td>
<td></td>
</tr>
<tr>
<td>COBIT</td>
<td>Control Objectives for Information Technology</td>
<td></td>
</tr>
<tr>
<td>COCO</td>
<td>Criteria of Control Framework, Canadian Institute of Chartered Accountants</td>
<td></td>
</tr>
<tr>
<td>COO</td>
<td>Chief Operating Officer</td>
<td></td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>COSEC</td>
<td>Company Secretary</td>
<td></td>
</tr>
<tr>
<td>COSO</td>
<td>Committee of Sponsoring Organisations of the Treadway Commission</td>
<td></td>
</tr>
<tr>
<td>COSO-ERM</td>
<td>Committee of Sponsoring Organisations of the Treadway Commission, Enterprise Risk Management Framework</td>
<td></td>
</tr>
<tr>
<td>COY</td>
<td>Company Name</td>
<td></td>
</tr>
<tr>
<td>CPA</td>
<td>Certified Public Accountant</td>
<td></td>
</tr>
<tr>
<td>CRIMS</td>
<td>Canadian Risk and Insurance Management Society</td>
<td></td>
</tr>
<tr>
<td>CRO</td>
<td>Chief Risk Officer</td>
<td></td>
</tr>
<tr>
<td>CSA</td>
<td>Control Self Assessment</td>
<td></td>
</tr>
<tr>
<td>CSA</td>
<td>Chartered Secretaries Australia</td>
<td></td>
</tr>
<tr>
<td>ERM</td>
<td>Enterprise Risk Management</td>
<td></td>
</tr>
<tr>
<td>EXO</td>
<td>Executive Responsible for Risk Management</td>
<td></td>
</tr>
<tr>
<td>FUN</td>
<td>Functional Arrangement for Audit and Risk Management</td>
<td></td>
</tr>
<tr>
<td>FYE</td>
<td>Financial Year End</td>
<td></td>
</tr>
<tr>
<td>GICS</td>
<td>Global Industry Classification Standard</td>
<td></td>
</tr>
<tr>
<td>GRC</td>
<td>Governance, Risk and Compliance (a movement from the United States)</td>
<td></td>
</tr>
<tr>
<td>HS&amp;E</td>
<td>Health Safety and Environment</td>
<td></td>
</tr>
<tr>
<td>IAU</td>
<td>Internal Audit Arrangement</td>
<td></td>
</tr>
<tr>
<td>ICA</td>
<td>Institute of Chartered Accountants</td>
<td></td>
</tr>
<tr>
<td>IFSA</td>
<td>Investment and Financial Services Association</td>
<td></td>
</tr>
<tr>
<td>IFRS</td>
<td>International Financial Reporting Standards</td>
<td></td>
</tr>
<tr>
<td>IIA</td>
<td>Institute of Internal Auditors</td>
<td></td>
</tr>
<tr>
<td>IPO</td>
<td>Initial Public Offering</td>
<td></td>
</tr>
<tr>
<td>abbreviation</td>
<td>description</td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>ISO</td>
<td>International Organisation for Standardisation</td>
<td></td>
</tr>
<tr>
<td>ISO 3000-1</td>
<td>The new international standard on risk management, released late in 2009.</td>
<td></td>
</tr>
<tr>
<td>KM</td>
<td>Knowledge Management</td>
<td></td>
</tr>
<tr>
<td>MENA</td>
<td>Middle East and North Africa</td>
<td></td>
</tr>
<tr>
<td>NACD</td>
<td>National Association of Company Directors</td>
<td></td>
</tr>
<tr>
<td>NASD</td>
<td>National Association of Securities Dealers</td>
<td></td>
</tr>
<tr>
<td>NYSE</td>
<td>New York Stock Exchange</td>
<td></td>
</tr>
<tr>
<td>OECD</td>
<td>Organisation for Economic Co-operation and Development</td>
<td></td>
</tr>
<tr>
<td>OH&amp;S</td>
<td>Occupational Health and Safety</td>
<td></td>
</tr>
<tr>
<td>REV</td>
<td>Revenue in A$ million</td>
<td></td>
</tr>
<tr>
<td>RMIA</td>
<td>Risk Management Institution of Australasia</td>
<td></td>
</tr>
<tr>
<td>SEC</td>
<td>Securities and Exchange Commission</td>
<td></td>
</tr>
<tr>
<td>S&amp;P</td>
<td>Standard and Poor's</td>
<td></td>
</tr>
<tr>
<td>SOX</td>
<td>Sarbanes Oxley Act (2002)</td>
<td></td>
</tr>
<tr>
<td>YRS</td>
<td>Years since incorporation</td>
<td></td>
</tr>
</tbody>
</table>
CERTIFICATE OF AUTHORSHIP

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the award of any other degree or diploma at Charles Sturt University or any other educational institution, except where due acknowledgment is made in the thesis. Any contribution made to the research by colleagues with whom I have worked at Charles Sturt University or elsewhere during my candidature is fully acknowledged.

I agree that this thesis be accessible for the purpose of study and research in accordance with the normal conditions established by the Executive Director, Library Services or nominee, for the care, loan and reproduction of theses.

Steven William Halliday

“Classical internal audit can no longer exist in a complex and rapidly changing world. In the old world independence was required to maintain the policemen role. Modern mature organisations no longer look at internal audit as policemen / compliance function, but as a valued partner and advisor. The next logical step in this more mature world is for the audit and risk to combine as valued forward looking partners, helping identify opportunities, manage blockers and assist with controls”

Quote from a Chief Risk Officer from an S&P/ASX 200 financial services company, interviewed in the qualitative sections of the research.
ABOUT THE AUTHOR

Steven Halliday is a sixty year old Australian Chartered Accountant. Steven has a Bachelor of Commerce from the University of Tasmania, a Master of Business Administration from the Edinburgh Business School, and a Master of Commercial Law from Deakin Law School in Victoria.

Steven has enjoyed a successful forty year career as a Chief Financial Officer, Strategic Planning Manager, Program Director, Chief Audit Executive, Chief Risk Officer, Chief Compliance Officer, Commercial Director and Company Secretary with international mining and utility companies.

More recently Steven is spending time in Abu Dhabi, where he is helping improve the corporate governance regimes (Audit, Risk, Company Secretarial, Compliance and Governance) within listed public companies in the Middle East and North Africa (MENA) region.

Steven commenced this doctorate in 2005, primarily driven by:

1. The growing importance of risk management in the international business fabric;

2. The reluctance of the internal audit profession to allow internal auditors to fully practice risk management. The author is concerned that this prohibition is keeping talented people out of executive management positions. The author also feels that this reluctance to adopt mature business practices may ultimately harm the audit profession.

3. The inability of small organisations to afford a Company Secretary, Chief Audit Executive, Chief Risk Officer and Chief Compliance Officer. Wrapping these roles into a single governance or assurance executive role, reporting to a board committee, seemed a persuasive solution; and

4. A strong belief that in the future, internal auditors will need to become experts in risk management, thereby adopting a more forward looking, strategic partnership with management.
ACKNOWLEDGEMENTS

To my supervisors Rod Duncan and Kay Plummer I am truly indebted. Your assistance throughout the project has been invaluable. Two areas in particular required persistence on your part. Firstly, helping me to scope this research into a “bite sized” project required a lot of energy. Secondly, ensuring that I constantly referred back to the research questions also taxed us at times, but with hindsight that was the perfect advice. Thank you for keeping me headed in the right direction.

I would like to acknowledge my previous employer Hydro Tasmania for assistance with funding this research. Contributions to the costs associated with doctoral workshops at Bathurst and Wagga Wagga were gratefully received. Study time allowed each semester also helped this project reach completion. The Assurance Group at Hydro Tasmania requires a special mention. You guys are a special team who put up with continual questions, proof reading of manuscript and often robust debates around the governance of risk management. To Peter Austen, Kevin Manderson, Jacky Purves, Esther Fox, Erika Koster, John Minchin, Donna Goodman and Tassie Strafkos my heart-felt thanks. Also thanks to Amanda Webb and Fiona Lewandowski, both my good friends and colleagues in the risk and governance world of the Middle East.

To Tony Hocking from ERMS Pty Ltd and Martin Farley of Farley and Associates thanks for your reviews of the survey questions and format. Designing a survey to fully capture the research objectives is a difficult and laborious process. Your final reviews and helpful suggestions gave me the confidence to complete and mail out the surveys.
To the Tasmanian risk managers who helped with pilot surveys and interviews, I am particularly grateful. Paul McTaggart, Leigh Burril, Mark Vincent, Alastair McDougall, Robert Kimber and Paul Oxley, thank you. To Maxine Glass who can magically produce two hundred letters from a mailing list, a big thank-you Max. Also to Margo Graeme-Evans and Michelle Nissink, thanks for helping find some very elusive references.

To the one hundred and two S&P/ASX 200 executives who responded to the survey, thank you once again. To the thirty five executives who agreed to be interviewed, I am grateful. For your help in pulling this research together, thanks also to the risk partners in the “Big Four” consulting firms. The survey respondents and interviewees are really what this study is all about.

Finally, I would like to dedicate this work to the three girls in my life, Jenny, Freya and Tegan. My career in commerce, finance, law, projects, risk management and internal audit has kept me away from home for long periods, dealing with other peoples’ problems. With the completion of this research, I will finally be able to focus on a list of jobs that are much closer to home. You are in my thoughts, always.
ABSTRACT

The primary research aim was to examine the organisational structure that is used to facilitate risk management in leading Australian companies, including an analysis of the tensions and strengths of integrating risk management with internal audit.

The study used a mix of quantitative and qualitative methods to explore the structure of risk management in leading Australian companies. A desk-top analysis explored the board committee arrangements across industry sectors. This was followed by a survey of the same companies to identify the reasons behind governance arrangements and why different models had been chosen. Finally, interviews were conducted to explore issues related to the governance of risk management.

The research found that 73% of S&P/ASX 200 companies govern risk management through the board audit committee. The reason for this was the natural synergy between audit and risk management. This synergy, a form of knowledge management, can be broken into three components:

1. The “circular flow” between audit and risk;
2. The “three lines of defence” model; and
3. The annual accounts as the scorecard for risk management.

Seventeen percent of Australian companies have a board risk committee separate from the audit committee. Separate risk committees were more prominent in the financial services sector where they originated from former credit and executive lending committees. The study found a number of problems with that model:
1. Over fifty percent of the banks indicated that they prefer the board audit committee to oversee risk;

2. Separate board risk committees tend to focus on market and trading risks rather than holistic risk management;

3. Separate board risk committees, having originated from credit or lending committees tend to be dominated by management;

4. Separate board risk committees find it difficult to capitalise on the synergy between audit and risk; and

5. Demarcation disputes often arise over committee boundaries with the audit committee.

The study found that 10% of S&P/ASX 200 companies have no board risk committee. The executives controlling these companies claimed that either the full board or an executive committee administered risk management.

Leading Australian companies are not experiencing problems with finding appropriately qualified directors for, and sufficient time at, board audit committee meetings. Across all S&P/ASX 200 companies, the Chief Financial Officer (CFO) was the predominant executive overseeing risk management. However, the Chief Risk Officer (CRO) is the leader in the energy, telecommunication, utilities and financial services sectors.

The survey work sought to establish the status of ERM implementation across the S&P/ASX 200 companies. Australian companies self reported sound awareness of ERM and the majority are well progressed with ERM adoption. The larger companies seem to be more advanced with their ERM maturity. There is no particular industry segment that is ahead of others on ERM implementation.
Full integration between internal audit and risk management was occurring in 30% of companies. Approximately 25% of S&P/ASX 200 companies used a partially integrated model where both teams report to a single executive.

Twelve percent had no risk management function and the remaining third had internal audit separated from risk management due to traditional independence concerns.

The maturity of the organisation, as defined by interviewees, emerged from the interviews as a strong driver for integration between internal audit and risk management. Interviewees noted that immature organisations required strong independence to administer a strict compliance role for the auditors.

Thirteen percent of companies had no risk management function and eighteen percent of the S&P/ASX 200 Australian companies had no internal audit function.

This study found that eighty two percent of S&P/ASX 200 companies have an internal audit function. This is a huge increase over previous Australian studies which found that only a third of companies had an internal audit function. It is clear that leading Australian companies now consider having an internal audit function as important.

This study also found that approximately thirty percent of leading Australian companies outsource their internal audit function. This is broadly consistent with previous studies.

Four broad models for risk management were outlined by the S&P/ASX 200 companies:
Traditional Independence Model: where the requirement for the internal auditor to be independent and objective dominates.

Current Merged Model: where risk management and internal audit both report through to the same executive.

Emerging Model: where the CRO had reached the executive team and internal audit is integrated with risk management.

No Internal Audit Model: where risk management, compliance or continual improvement functions work as de-facto internal auditors.
CHAPTER ONE - INTRODUCTION

1.1 INTRODUCTION

The global corporate collapses of the late 1990’s and early 2000’s placed the concept of risk management firmly on the governance agenda (Bugalla, Kallman, Lindo & Narvaez, 2012). Additional regulatory requirements such as the Australian Securities Exchange, Principles of Good Corporate Governance and Best Practice Recommendations (ASX Principles) mean that boards of directors are grappling with the implementation of risk management. The recent global financial crisis, which has brought down household names such as Lehman Brothers and ABC Learning Centres, has intensified this situation.

In the aftermath of the recent corporate collapses, numerous government initiatives have been proposed for improving corporate governance with significant emphasis placed on the role of risk management (Subramaniam, Zhang & McManus, 2009, p 316). In the United States the failure of Enron and WorldCom led to the introduction of the Sarbanes-Oxley Act (SOX) and the Committee of Sponsoring Organisations Enterprise Risk Management (COSO-ERM) risk framework (Von Nessen, 2003, p. 192).

In Australia, McClelland and Stanton (2004) saw the collapse of HIH and OneTel as having triggered the Ramsay Report, CLERP 9 and changes to Australian Securities Investment Commission (ASIC), licensing requirements. Also, the introduction of the ASX Principles in 2003, and in particular the 2007 revision, brought a heavier focus onto the role of risk management.

The Cadbury Commission report in the United Kingdom established “a Code of Best Practice for all UK public companies to adopt and address in their annual reports to shareholders” (Lam & Kawamoto, 1997, p. 33). In addition the Turnbull Committee has issued guidelines for non-financial and risk controls.
These are all part of the Combined Code which today forms the backbone of the United Kingdom’s corporate governance legislation.


The recent global financial crisis has perpetuated this rate of change in governance and risk management. As described by Protiviti (2008) the financial community has sought changes to:

- the operating model for the finance industry;
- Basel II recommendations on banking laws and regulations issued by the Basel Committee on Banking Supervision;
- liquidity management;
- stress testing;
- executive compensation; and
- the role of rating agencies.

The Chartered Secretaries Australia (CSA) has promptly responded by considering changes to regulation. In January 2009 they reported that “nearly two thirds of those working in governance believe that the financial markets should be regulated globally because of the recent economic upheaval” (p. 1).

Internationally, all these changes have been aimed at strengthening risk management practices and enhancing the internal control environment. These legislative changes require that modern listed companies have a well developed risk management regime. Such a regime starts with the board governance arrangements, including the board committee overseeing risk management. The structure at board level then flows down to executive levels and finally to the risk management arrangements at the organisational or functional level. Risk management is a new and evolving discipline.
Rapidly changing regulation is increasing the focus on risk management, hardly allowing time for the discipline to find its place in corporate governance.

Companies struggling with the implementation of risk management structures are using different models and are experimenting with various structural alternatives. An investigation of these alternatives underpins this thesis.

This research is about the governance structures that support risk management in leading Australian companies. Using the Standard and Poor’s / Australian Securities Exchange 200 companies (S&P/ASX 200), the corporate governance placed over risk management at board committee, executive and operational level was investigated.

The research was required because boards and executive management are grappling with governance questions around risk management and are trying to find where risk management fits into the modern organisation. The models that Australian companies are adopting to govern risk management have been identified. The levels of integration between the two related disciplines of risk management and internal audit were also investigated.

The research literature shows a growing integration between the internal audit and risk management functions in the United Kingdom (Richmond, 2006), the United States (Gramling & Myers, 2006) and Australia (Moloney, 2005). Combined board risk and audit committees have become commonplace while some companies, especially banks and derivative traders, have set up specific board risk committees, in addition to audit committees, to monitor specialised aspects of risk. These activities are effectively agency theory controls that seek to align the interests of the agent (management) with those of the principle (the shareholders).
Institutional theory tells us that if internal audit and risk management are moving closer together overseas, then Australian firms will tend to adopt similar models as a method of seeking legitimacy (DiMaggio & Powell, 1983).

Given the smaller size of Australian firms, they might choose to integrate board committees and operational functions as an efficiency measure when faced with the escalating costs of regulation.

Contingency theory (Lawrence & Lorsch, 1967) shows how the environmental factors facing a firm can shape the structure, controls and agency responses.

Are separate board risk management committees in the finance industry a response to environmental risk factors? Does signalling theory, the need to overtly flag to the market the steps an organisation is taking to manage risk, explain why banks might set up board risk committees, separate from the audit committee.

Is the growing integration of internal audit and risk management an example of the more contemporary knowledge management theory? Audit and risk both use the common languages of risk management, probability and statistics. They also share many of the traits required from the tenants of knowledge management.

Risk management is now arguably mandated by progressive international company regulation. To the authors’ knowledge, this research will provide the first overall study of the structure and governance over risk management in Australia.

1.2 THE NEED FOR THE RESEARCH

The author has enjoyed a forty year career in the commerce, legal and governance arena. Over that period a number of unanswered questions faced risk management practitioners and have motivated this study. These practical questions included:
1. Why is risk management growing in importance and what is the relationship between that discipline and internal audit?

2. Why do Chief Audit Executives (CAE) earn less than Chief Financial Officers (CFO) and Chief Risk Officers (CRO) when often, they have the same training and qualifications?

3. Why does the Institute of Internal Auditors (IIA) define areas of risk management that internal auditors must avoid (IIA UK and Ireland, 2004)? These prohibitions push the role of the CAE into a much lower and less persuasive position?

4. Can smaller companies combine the role of Company Secretary (COSEC), CAE, CRO and Chief Compliance Officer (CCO) into a single multi-skilled professional? and

5. Will internal auditors in the future need to be trained in risk management, thereby moving from a backward looking compliance view to a more strategic, forward looking perspective?

Unlike internal audit, where a substantial body of knowledge has directed professional practice over time, the management of risk has a short history, limited research and a paucity of academic literature.

Boards are asking questions about where risk management fits into the corporate fabric. Do we need a risk committee as well as an audit committee? How should the management of risk be shaped at executive level? Can risk management be outsourced and do we need a CRO?

These questions are difficult to answer because risk management is a newcomer to the corporate agenda, there is limited research in the area and the risk profession is threatening long established traditions. The KPMG 4th Annual Public Company Audit Committee Member Survey (2009, p.5) found that:
Virtually all boards today are taking a hard look at how the company manages risk, and how the board oversees that process. Three out of four respondents said their board audit committee is reassessing risk management oversight as a result of the financial crisis.

In a similar vein, executive managers are trying to cope with where risk management fits into the organisation. Can risk managers report to CFOs, Chief Operating Officers (COO) and COSECs, or will the executive inner sanctum admit a new breed of risk professional? How do we control risk management from a central coordinating point when it is the responsibility of every employee and manager across the organisation? Can smaller companies combine the roles of CAE, CRO and CFO to reduce costs and increase effectiveness?

Subramaniam, Zhang & McManus (2009, p. 6) felt that:

Further understanding of the establishment of risk management committees is important as it leads to a more comprehensive understanding of the factors that enhance or act as barriers to setting up proper risk management structures within an organisation.

Professional institutions and industry associations are not insulated from this debate and are heatedly competing for the lead role in this new risk and compliance world. The Institute of Internal Auditors (IIA) is promoting a much greater role for its members in risk management. However, the IIA stops short of allowing overall control of risk management due to traditional concerns over the independence and objectivity of auditors (IIA UK and Ireland, 2004). This has allowed the Risk Management Institute of Australia (RMIA) and the Australian Compliance Institute (ACI) to gain inroads into this new profession at the expense of the IIA. In the United States, a governance, risk and compliance (or GRC) movement is rapidly evolving, a movement without the traditional links to accounting or auditing.
Professional organisations also need to understand the training and skill sets required for their members. Will future internal auditors require risk management and compliance training?

Will the IIA need to increase its focus and resource spend on defending the profession against the inroads being made by risk management professionals?

Regulators are demanding greater board control over the governance of risk management. Neither a Australian Financial Services Licence (AFSL) nor a Australian Prudential Regulatory Authority (APRA) approval can be granted without evidence of board oversight of risk and a well developed risk management system.

Shareholders worry about governance structures and rating agencies are now rewarding companies with solid risk and compliance systems by issuing more favourable credit ratings which lead to lower costs of capital.

Universities are concerned about curriculum with questions such as, do we need to include a risk management unit in our Bachelor of Commerce program? Do we need to include a regulatory compliance unit in our undergraduate law program?

Understanding what sort of company is adopting enterprise risk management (ERM), why they are using a particular framework and in what manner it is being used has implications for future efficient implementation of risk management systems. Discussions with Standards Australia have indicated that such research would be valuable to them as the new ISO 31000 is adopted.

The research sought to answer these practical questions and highlight the governance practices leading Australian companies are applying to risk management. The project provided an up to date synthesis of the current situation, identified the drivers behind the status quo and some important trends for the future.
1.3 DEVELOPING THE RESEARCH OBJECTIVES

Chapter Two reviews the scarce literature on risk management and investigates some of the controversial debates occurring on this contemporary subject.

The gaps in the literature are converted into four research objectives. Firstly, a primary, overarching research aim, which then breaks down into three research objectives that underpin that primary question.

The primary research question addresses the organisational structure of risk management in leading Australian companies and how that structure relates to the integration of risk management with internal audit:

To examine the organisational structure that is used to facilitate risk management in leading Australian companies, including an analysis of the tensions and strengths of integrating risk management with internal audit.

To flesh out the primary question in a little more detail requires consideration of the governance structures utilised in leading Australian companies. These governance structures are born of agency theory and are part of the controls that the owners or principals place over management, the agent. The first and highest level of governance structure is at the board and board committee level. The second level of governance is that of executive management. The final level of governance is the structure at the operational or functional level. The first research objective that flows from the primary research question above:

To investigate how risk management is structured at the board committee, executive management and operational levels in leading Australian companies.

This objective gives some direction when looking at the structures for risk management in leading Australian companies.
The gaps in the literature point to areas where this research can make an original contribution to increasing professional understanding of both risk management and internal audit.

A second research objective deals with the relationship between risk management and internal audit in Australian companies. That objective is:

To establish what levels of integration exist between internal audit and risk management in leading Australian companies.

One of the predominant themes of this research is the extent to which the functions of risk management and internal audit are being integrated. While there is some literature on this trend at the international level, there is little that has been published on the Australian situation.

Finally, the third research objective that flows from the overarching research question discussed above, relates to models for the governance of risk management in leading Australian companies:

Can a number of models for risk management be identified in the population of the S&P / ASX 200 Australian companies?

The models predict the likely make up of the governance of risk management at three levels, the board, executive and the functional or operational level.

1.4 RESEARCH METHODOLOGY

The research methodology is designed to address the research questions on the board committee and organisational structures that sit over risk management in leading Australian companies. This includes the relationships and links between the governance of internal audit and risk management and contemporary thinking on the interaction between these functions.
Using a mix of quantitative and qualitative methods, the research explores aspects of risk management in a manner that ensures the validity and reliability of the study, with each section building on the previous and providing validation and triangulation at each stage.

The S&P/ASX 200 index is chosen as being representative of leading Australian companies. The study does not assert that this population is representative of all Australian companies but suggests that being included in the S&P / ASX 200 is something that most listed companies aspire towards.

The question of oversight for risk management at board level is addressed by a desk-top analysis of the annual reports of a selected population of Australian companies. The desk-top analysis seeks to answer questions about the audit and risk committees in relation to various company characteristics. The data-set of each company includes revenues and industry classification. The status of the board risk and audit committee arrangements is also included.

The information gained from the desk-top analysis underpins the next stage which looks at the reasons why companies choose a particular board risk oversight model. That stage also reviews how companies are managing the risk management function at the level below the board committee.

To extract information on the next level of governance, a survey of the same S&P / ASX 200 companies is required. The survey instrument asks questions on:
• size – to triangulate with the desk-top analysis;
• board audit and risk committee structure – to triangulate with the desk-top analysis;
• why such a board structure was chosen;
• the maturity of the ERM system adopted by the company;
• the executive presiding over risk management;
• existence of a risk management unit (in audit or in a separate function);
• the impact of “independence” on the governance structure; and
• whether the internal audit function was co-sourced or outsourced.

Since a survey was used that involved respondents providing somewhat confidential information about their companies, ethics became a prime consideration. Approval was gained from the Charles Sturt University Ethics Committee (see Appendix Fifteen).

The survey achieved a response rate of fifty nine percent which is quite remarkable for this type of research. This confirms the interest in the subject and the need for this research.

The questions arising from the desk-top and survey analysis feed into the next stage where qualitative interviews are undertaken to document the management perspective on the key issues.

After the interviews were completed the study had quantitative, statistical and descriptive outcomes on the governance framework over risk management in leading Australian companies. The desk-top analysis showed the board committee structure by revenue and industry classification. The survey data-set explains why a particular board committee structure was chosen and how risk management was structured under the board committee level.
The interviews with selected participants provided further insight into why particular models were chosen. Data analysis of the interviews is undertaken by looking for common groupings of thoughts, comments and themes. The respondents’ answers to each question are dissected into different elements and summarised using thematic analysis.

1.5 FINDINGS

The percentage of S&P / ASX 200 companies that are governing risk management through the board audit committee is provided. The reason for choosing this model is discussed with respondents and broken into a number of agency components. The “synergy” between internal audit and risk management, which is driving integration, was defined by the interviewees.

The number of S&P / ASX 200 companies choosing to adopt a separate board risk management committee was outlined. The reasons for adopting this model are discussed, particularly in relation to industry classifications and the impact of signalling theory. The problems that result from separating these committees are also outlined by the respondents.

A small percentage of S&P / ASX 200 companies do not have a risk committee at board level. This situation was investigated and the reasons for the lack of risk management were discussed.

With risk management providing an additional load for board audit committee members, key writers have suggested that directors are struggling with that increased workload. That issue was investigated and the Australian solution to that problem was outlined.

The extent of adoption of ERM by S&P / ASX 200 companies was investigated and discussed. This is the first time that a Beasley (2005) style of ERM maturity classification has been attempted across Australian companies.
The executive structure over risk management in the S&P/ASX 200 was outlined. The role of the CFO, CRO and CAE was documented. These findings were important in developing the later models for risk management.

The extent of integration between internal audit and risk management was explored, together with the reasons for such integration. The S&P / ASX 200 companies’ attitude to independence was also discussed.

To help explain the relationship between internal audit and risk management, the extent of outsourcing and co-sourcing was investigated. The type of companies that tend to outsource was also reported.

Companies with no internal audit function were documented and noted. The reasons for this model were revealed and the relationship to risk management was discussed.

Finally, bringing all of the above together and drawing on interviews with governance executives, four broad models for risk management were outlined within the S&P / ASX 200 companies. These models are discussed in terms of reporting lines, independence, maturity and whether they were forward (strategic) or backward (compliance) oriented.
CHAPTER TWO – LITERATURE REVIEW

2.1 INTRODUCTION

The primary research aim addressed the structure of risk management in leading Australian companies and how that structure relates to the integration of risk management with internal audit:

To examine the organisational structure that is used to facilitate risk management in leading Australian companies, including an analysis of the tensions and strengths of integrating risk management with internal audit.

The purpose of this chapter was to extend the primary question by:

1. Developing a theoretical framework that can be used in this study to explore the research objectives;

2. Reviewing the contemporary literature, contentious issues and current debates on the increasingly important subject of risk management. The review identified the issues and research gaps that underpinned the study; and

3. The primary research aim was extended into a manageable set of research objectives, based on the issues identified from the literature.

The following section outlines the format for this chapter.

2.2 OVERVIEW OF THIS CHAPTER

The first section of this chapter identifies the theoretical frameworks that will underpin the examination of risk management structures in Australian companies. Agency theory is introduced as a motivation for aligning the expectations of owners and managers. That theory impacts on the choice of structures and governance adopted by Australian companies. Institutional theory is then discussed in the context of whether Australian companies might be followers or leaders in regard to contemporary risk practices.
Contingency theory is introduced as a possible explanation for the impact of environmental factors on the determination of risk structures. Signalling theory is also outlined as a potential reason why some companies might set up specific risk structures to flag to the market that they have a particular focus on risk management. Knowledge management (KM) is discussed as a possible explanation for the synergies between internal audit and risk management. Those synergies appear to be driving integration. Finally, power theory is introduced as an alternate explanation for synergy and life-cycle models are used to underpin governance arrangements at different stages of corporate development.

Having outlined a theoretical basis for the study, the chapter then examines the literature on some of the more controversial issues that currently surround the governance of risk management.

Firstly, because risk management structures form part of governance, corporate governance is defined. The current debate concerning governance as a board imposed process versus a measurable outcome, is discussed (Clarke & Dean, 2007). This helps scope the research and defines what is included and what is excluded from the research proposal.

Next, the need for good governance is outlined and the relationship between governance and director liability is then reviewed in the light of recent court decisions, including the James Hardie Limited action. The concept of director liability is a strong driver for implementing risk management systems.

The literature on the role of the board committee is examined and considers both the board audit committee and the board risk management committee. While the majority of companies govern risk management through the board audit committee, some companies have set up separate board risk committees.
Which of these two models is the preferred practice is a debate currently facing those wrestling with the governance surrounding risk management.

Studies have also identified that problems with the skill sets of directors and timing issues regarding committee meetings are both contributing to debate over the structure of board committees.

The extent to which Enterprise Risk Management (ERM) is being implemented by companies is then covered as this variable will impact on the chosen risk management structure. Problems associated with the implementation of ERM are also outlined. That leads to a discussion of the executive structure over risk management both internationally and in the Australian context. The roles of the CFO, the CRO and the CAE are introduced at that stage. Those executive roles are competing for the right to oversee risk management in the international business arena.

Across the globe, the disciplines of internal audit and risk management are showing growing levels of integration. This is not however occurring smoothly, given the Institute of Internal Auditors (IIA) requirement for internal auditors to remain independent and objective. Integration between internal audit and risk management is introduced using the paradigm shift first identified by McNamee and Selim in 1998. This is followed by a discussion of possible reasons for the merging of these two related disciplines as a result of the synergies that bind those two functions together. Integration is the subject of limited research overseas, and has not yet been the subject of any significant research in Australia. Studying the integration between internal audit and risk management is a fundamental aim of the research.

The governance structure over internal audit is then discussed, followed by the controversial independence issue surrounding that topic. That leads to a discussion of the role of internal audit in risk management, a subject also experiencing significant debate.
In many countries, the distinction between risk management and internal audit is becoming blurred.

Finally, the debate on whether internal audit should be co-sourced or outsourced is examined in the context of the integration between audit and risk management.

A table outlining the main researchers in the risk management discipline is included as Appendix Fourteen. That table outlines the more significant writers for each debate noted in this chapter and includes their objectives, methodology and findings.

Using the issues debated in the literature and the gaps identified, the primary research question is then expanded into three research objectives. Those objectives are aimed at finding answers to what is happening to the structure and governance of risk management in Australia, where it is heading and whether a paradigm shift to a new integrated model has started to emerge.

### 2.3 THEORETICAL FRAMEWORKS

The research is aimed at the board committee or governance structure over risk management, a relatively new board function. That structure cascades down to the executive management oversight of risk management then down to the functional arrangements for risk management. The theories underpinning this research need to explain and/or predict governance arrangements, explain the rationale behind new management structures and outline the drivers for functional arrangements. Given the different environments facing S&P/ASX 200 companies, i.e. industry classification, age, relative wealth and life-cycle, a theory explaining environmental impacts is also required.

The literature on governance structures shows that agency theory is the main paradigm used in prior studies, and the need for a multi-theoretic approach is recommended (Subramaniam et al, 2009, p 320).
Since risk management is a newcomer to governance, the manner in which it is adopted by other leading companies, or peers, will impact the functional adoption.

Institutional theory provides an insight into how companies in related fields often adopt similar governance structures. These similarities arise from pressure by powerful stakeholders, copying behaviors or peer pressure (DiMaggio and Powell, 1983). Also power theories (Lukes, 1974 and Clegg, 1989) are closely related to institutional theory and may explain the adoption of risk structures by influence from powerful stakeholders.

Contingency theory, as used by Carey, Subramaniam & Ching (2006) takes environmental factors into account when determining governance structure. The banking industry is a heavy adopter of board risk committees. There may be an environmental factor, the risky nature of derivatives that is driving such a structure. Signalling theory has also been used to explain why different governance structures have been adopted. Liebenberg and Hoyt (2003) use signalling theory to show that in some industries, the signalling of robust risk arrangements to the market, was driving the appointment of CRO’s. Another important environmental factor, the life cycle of the company, was also considered. The stage of life-cycle development will impact on the risk structure arrangements. Auzair and Langfield-Smith (2005) found that mature and cost leader firms chose a more bureaucratic form of management control (governance) system as compared to start-up companies.

Finally, a theory was required that explained the close links between the disciplines of internal audit and risk management. The growing integration of these functions as noted by Hass, Abdolmohammadi & Burnaby, 2006, Allegrini, D’Onza, Paape, Melville & Sarens, 2006 and Cooper, Leung & Wong, 2006 may be related to the similarities in using a common knowledge as discussed in Grant (1996) and Nonaka and Takeuchi (1995).
In order to address the primary research question appropriate theoretical frameworks needed to be considered. The following theoretical structures were useful in developing the research objective:

- **Agency Theory:** provides some insights into the governance structures that boards place over risk management;

- **Institutional Theory:** provides reasons why international risk management practices are starting to appear in the Australian business community;

- **Contingency Theory:** helps establish why different risk management models are being used by companies in different situations;

- **Signalling Theory:** explains why some risk management models have been chosen to signal governance practices to the wider financial market;

- **Knowledge Management:** provides an explanation for the growing integration between internal audit and risk management, and could underpin the synergies between audit and risk management.

- **Power Theory:** introduces a political explanation for the synergy between internal audit and risk management; and

- **Life-cycle Theory:** outlines an explanation for the governance structures at different points in the company life-cycle.

The next seven sections provide a brief overview of each of these theoretical frameworks.

### 2.3.1 Agency Theory

The governance overlay for risk management cannot be investigated without discussing agency theory. Agency theory provides the primary explanation as to why governance policy, process and procedures are implemented by boards of directors.
Jensen and Meckling (1976, p.308) define an agency relationship as a contractual arrangement. The principal, the owner represented by the board, contracts with the agent, usually management, to operate the venture, ideally in the best interests of the principal. However, the agent may act in his or her own best interests, which may not align with those of the owner.

This misalignment of interests results in agency costs. Agency costs include not only the costs of contracting but also the costs of lost wealth due to the agent making decisions that benefit the agent but disadvantage the principal (Jensen & Meckling, 1976). Agency costs also include the costs of governance, the monitoring costs of internal audit, risk management and compliance. These costs are incurred to ensure that the interests of the principal, often the board, are aligned to those of the agent, management.

Fama and Jensen (1983, p.301) make this concept a little clearer. They argue that often the agent will make decisions in an environment where they are not subject to the wealth effects, creation or destruction, of such decisions. Fama and Jensen (1983) term this “the separation of decision and risk bearing functions”. This means that an agent can make a decision that will benefit the agent in the short term, but which might damage the principal, and indeed the company, in the longer term.

Jensen and Meckling (1976) put forward two methods of reducing agency costs:

1. the use of monitoring mechanisms or governance oversight, such as risk management and internal audit, to align both the interests of principal and agent; and

2. using incentives to bring the interests of the principal and agent into alignment.

The governance mechanisms that companies place over risk management activities can be traced back to agency theory.
In this context governance is seen as a necessary contractual mechanism that is designed to monitor management behaviour.

Cohen, Krishnamoorthy and Wright (2002, p.579) support this theme of board governance reducing agency costs, “directed primarily towards monitoring and control, evaluation of performance, global risk management and management recruiting and compensation”.

Jensen and Meckling (1976) found that the separation of ownership and control give rise to agency problems. Both risk management and internal audit are monitoring mechanisms that allow absent owners a degree of confidence that internal controls are operating and risks are being addressed.

Cohen et al (2002) use agency theory to study the impact of boards and board sub-committees on the external audit process. In that study they used semi-structured interviews with 36 auditors to investigate views on corporate governance. Cohen et al found that:

1. corporate governance mechanisms are often strongly influenced by management, a finding that is inconsistent with the agency theory perspective of independence;

2. audit committee members are often lacking in key financial literacy skills, the committee may be subservient to powerful management and may only be symbolic in nature; and

3. audit committees may lack sufficient power to be a strong governance mechanism.

Agency mechanisms, such as corporate governance, are supposed to align the interests of the owners with management. It seems however, that these controls can become hijacked by management or by ineffective or skill deficient board committees (Cohen, 2002). In this study the skills of Australian directors on board committees were investigated.
Situations where management risk committees were adopted in preference to board risk committees are also discussed, particularly in the finance industry and where some companies chose not to adopt a board risk committee.

Subramaniam et al (2009) used agency theory to research the factors associated with setting up a board risk committee in Australian companies. Data was collected from the annual reports of the S&P/ASX 300 Australian companies, using a desk-top analysis. That study looked at: the proportion of non-executive directors; chairman independence; board size; industry type; organisational complexity and financial leverage. Logistic regression was then applied to find that companies with separate board risk management committees are likely to be the larger companies, have higher financial reporting risk and lower organisational complexity. That study also found a positive relationship between board size and chairman independence with the existence of a risk committee.

Agency theory has been used to explain the rationale behind, and reasons for, the existence of board committees. Ruigrok, Peck, Tacheva, Greve and Hu (2006) and Benz and Frey (2007) found that, in general, board committees lead to stronger monitoring and control mechanisms and hence lower opportunistic behaviour by management. This appears to conflict with Cohen’s finding that board committees might be strongly influenced by management. However, that might be due to methodological and sampling issues. In the Cohen study, interviews were only conducted with 36 auditors, whose views may not be representative of the companies that they audit. The Ruigrok et al and Benz and Frey findings are broadly valid. The use of board audit and risk or board risk committees is likely to be more developed in companies subject to higher agency costs, that is, larger or more complex firms. In this study, the size of S&P/ASX 200 companies was a key variable.
Kleffner, Lee and McGannon (2003) used agency cost related factors to examine the use of ERM by Canadian companies. That study looked at regulatory guidelines, size, industry grouping and the placement of ERM within companies.

The study found that energy companies, firms with a dedicated risk management function and firms with a reliance on the Toronto Stock Exchange guidelines all had a stronger ERM presence.

Agency theory has also been used to identify factors associated with the implementation of ERM. Beasley, Clune and Hermanson (2005) used logistic regression analysis to find out which agency related factors are correlated with successful ERM implementation. They found a positive correlation between ERM implementation and the presence of a CRO, board independence, CEO and CFO support for ERM, the presence of a Big Four auditor, entity size and entities in the banking, education and insurance sectors.

In this research, the implementation of the ERM process, within each S&P/ASX 200 company was investigated as that level of maturity might be a key driver of board, executive or functional structure.

Agency theory was also used by Liebenberg and Hoyt (2003, p.43) to suggest that ERM might be used effectively to mitigate the Fama and Jensen (1983) risk shifting or asset substitution problem. Shareholders can profitably alter the firms risk profile after securing long term finance. Debt providers anticipate this behaviour and price such behaviour into the cost of debt. That study found that: “ERM systems provide a way for firms to make a credible commitment against such behaviour because they facilitate better disclosure of the firm’s risk exposure”.

Christopher, Sarens and Leung (2009) used the relationship between agency theory and internal auditor independence in a study that reviewed auditor independence in Australian companies. The study found that organisations operate in an environment that compromises audit independence.
In a similar study Goodwin-Stewart and Kent (2006) used agency cost related variables such as risk management committees, risk managers, industry, size and business structure to investigate the use of internal audit by Australian companies. The study found strong links between company size and a commitment to risk management in the decision to engage in internal audit activities.

As can be seen above, agency theory provides an explanation for governance and potential governance structures. Control is vested by the shareholders, the principal, to the board and management become the agents. The shareholders use the external auditors for assurance over satisfactory board performance.

The board, in turn, uses internal audit and risk management, through the audit committee, to provide assurance about the satisfactory performance of management.

The relationship between agency theory and signalling theory was investigated in this research. Is risk management being adopted to signal a strong agency response to key stakeholders? Do financial firms want to signal to the market and regulators a strong agency response to their core business of risk management?

The factors impacting on agency theory through agency costs were important in this research. The structures adopted and behaviours involved depend on the size of the organisation, which industry classification and even the period of incorporation or newness of the entity. In this research agency theory was used to help explain the differences between risk management structures. Agency theory was also used to test which agency related factors such as size, and industry grouping, impact on the risk structure chosen.

2.3.2 Institutional Theory

For this research, a theory was required that helped explain why leading companies tend to adopt practices that are used by other high performing organisations.
Institutional theory provided some guidance on the board committee structure adopted by Australian companies.

Institutional theory helped explain why companies in related fields, for example financial services, often adopt similar governance structures. Legitimacy and signalling theories showed how reporting and disclosures are adopted to signal legitimacy to the broader stakeholder population.

Institutional theory takes this one step further and looks at the forms and structures that might be adopted to cement legitimacy.

Institutional theory, as developed by Meyer and Rowan (1977), DiMaggio and Powell (1983) and Zucker (1987), presents an argument that the broader population of companies will tend to adopt the key governance characteristics of similar leading organisations as a legitimacy seeking measure.

DiMaggio and Powell (1983) are key developers of institutional theory. They sought to explain why organisations start out with very diverse structures, but these structures tend to become more homogenous as the organisational field develops over time. DiMaggio and Powell (1983) found that over time the structures and reporting processes adopted by organisations converge to align with the norms of society and also the expectations of powerful stakeholder groups.

DiMaggio and Powell (1983, p 149) termed this convergence as isomorphism, “a constraining process that forces one unit in a population to resemble other units that face the same set of environmental conditions”. The authors identified three types of isomorphism: coercive; mimetic; and normative.

Coercive isomorphism posits that organisations will change their structures and practices due to pressure applied by powerful stakeholders who are important to the organisation’s existence (DiMaggio & Powell, 1983).
This could explain why Australian companies tend to adopt the governance structures and voluntary reporting required by both the ASX Principles and institutional shareholders. It would also partly explain the growth in risk management since Standard and Poor’s have started to include ERM factors into the manner in which credit is rated.

The second isomorphism outlined by DiMaggio & Powell (1983), mimetic isomorphism, occurs where an organisation copies other organisations in an effort to seek legitimacy. Benchmarking (Zairi, 1998) is a good example of this behaviour, where organisations seek to be leaders by implementing similar practices to those adopted by acknowledged leading companies.

DiMaggio and Powell (1983, p.151) see uncertainty as the primary driver for mimetic isomorphism, “Uncertainty is a powerful force that encourages imitation. When organisational technologies are poorly understood, when goals are ambiguous, or when the environment creates symbolic uncertainty, organisations may model themselves on other organisations”.

This theory may explain why risk management, which was a new discipline twenty years ago, has developed into the more standardised ERM system of processes and controls evident in modern organisations. This theory may also explain the suite of risk management controls that are evolving as both regulation and director liability becomes increasingly complex.

Normative isomorphism results from peer pressure. This may arise from professional guidance in the case of corporate reporting, industry association recommendations or even academic debate on particular issues. That concept might help explain why the ASX, the IIA and the Risk Management Institute of Australia (RMIA), all have varying degrees of influence over the structure of risk management in leading Australian companies.
Meyer and Rowan (1977) add to institutional theory by stating that firms will seek legitimacy even if the practices are not particularly useful. This might explain why certain board characteristics, such as composition, structure and membership, are adopted when the link between those characteristics and performance is still hotly debated. According to Meyer and Rowan, as firms grow in size and complexity, they tend to adopt rationalised formal structures that stem from public opinion, important stakeholders, social prestige and the educational system. Often these structures, which Meyer and Rowan say can function as myths, are adopted to avoid illegitimacy.

The legitimacy seeking process, isomorphism, discussed by DiMaggio and Powell (1983) would predict that Australian companies will adopt the overseas practice of governing risk management through the board audit committee. Also Australian companies will integrate internal audit with risk management, in a manner similar to the overseas experience.

Deegan (2006) indicates that institutional theory is relevant to research as, “it provides a complementary perspective to both stakeholder theory and legitimacy theory”. Institutional theory has been used by both organisational analysts and accounting researchers. Covaleski and Dirsmith (1988) adopted an institutional perspective to examine how key stakeholders impacted on the university budgetary process. That study used working papers, formal budget submissions and in-depth interviews with the main budget players to gather data. They found that specific individuals invent and then articulate institutionalized expectations regarding policies and procedures. That study also found that the game of institutionalization appears to be played on a stage fraught with power and self-interest.

Rollins and Bremser (1997) based a review of SEC enforcement actions on institutional theory. The study sought insight into auditor reputation based on whether audit firm characteristics related to SEC enforcement actions.
Using a logistic regression model, that study found that audit firm size, CPA membership and the existence of disclosure violations all impact on auditor reputation. That reputation has a brand name aspect through which both auditors and the SEC are seeking social legitimacy. The study showed that the largest auditing firms were disciplined less frequently and received lighter penalties. Institutional theory suggests a possible explanation of the SEC’s enforcement activities. Institutional theory predicts that brand name auditors will be treated differently by a regulatory agency.

Brand name auditors have formal structures, policies and procedures to demonstrate conformity to institutional rules and constituent expectations, and they have greater auditing expertise than most no-name brand auditing firms. They have attained a certain amount of social legitimacy and power. Confidence associated with brand name auditors has influenced the capital markets and regulators.

The above studies show that in the world of institutional theory, perception is important. Both the university budget process and the United States peer review programs involved game playing aimed at portraying a professional image, whilst behind the scenes, political manipulation held sway. In this study, the views of senior managers were sought on the perception underlying board audit and risk committees, the CFO role and the integration of audit and risk. The prevailing view that having strong board committees leads to better business outcomes, a perception, might be compromised by dominant management, a weak or unskilled board committee or arrangements that signal legitimacy, but in reality add little value.

In this study, institutional theory helps explain why a board elects to govern risk management through either a separate board risk committee or through the audit committee. Powerful regulating influences such as the Australian Prudential Regulation Authority (APRA) and the Australian Securities and Investment Commission (ASIC) may assert coercive isomorphism to promote a favoured model.
The move to implement ERM may be a form of mimetic isomorphism. With the S&P/ASX Principles requiring a greater focus on risk management, firms will turn to one another for assistance with finding the most efficient system with the lowest cost.

The elevation of the CRO to the executive team in the banking environment may be a symbolic myth, aimed at rationalising a formal structure to legitimise the organisation.

The risk management institutions could be promoting the concept of ERM to reinforce their rules and procedures into the business environment. If a company chooses not to adopt ERM they will appear more vulnerable or even negligent by not ceremonially adopting what could be a powerful myth.

The functional structure of risk management may be defined by the coercive isomorphism promoted by the internal audit profession, where rules dictate the separation of internal audit from risk management. Later in this chapter, it will be shown that the internal audit profession is seeking its role in the extent to which internal auditors can become involved in risk management. The IIA accepts that audits must be risk based and that internal audit and risk management has many synergies. However, the inclusion of risk management in the audit world poses a threat from competing organisations in the risk and insurance professions, organisations seeking additional roles and expertise for their members. The inclusion of risk management with internal audit also threatens to impact on audit independence, a cornerstone of the internal audit profession.

Alternatively, mimetic and normative isomorphism will see the integration of risk and audit functions as a blend of two disciplines that are heavily interwoven. Internationally accepted regulations such as SOX, Turnbull, Dey and the ASX Principles bring risk management and internal audit closer together.
The IIA common body of knowledge (CBOK) project (2006) also shows clearly that internationally, risk management and internal audit are converging. This study explored, in detail, the ASX 200 companies' attitudes to this integration question and some of the practical realities of operating in such an environment.

The Australian S&P/ASX 200 companies were chosen as the full population of good practice companies for this study. Some of these companies have overseas parent companies that dictate the governance structural arrangements. This is an example of coercive isomorphism, or powerful stakeholders exerting influence.

The influence of powerful parents is captured throughout chapter four, where the findings from the research are presented.

This research also required a theoretical basis to help explain why different companies will set up a variety of governance mechanisms, depending on the environmental factors facing the company.

### 2.3.3 Contingency Theory

Contingency theory is a theory of management developed in the 1960’s. The theory is based on the work of Joan Woodward (1958) and Burns and Stalker (1961) and it replaced the earlier bureaucratic and scientific approaches developed by Weber (1958) and Taylor (1939) respectively.

Contingency theory suggests that management structures are aligned with or fit with the technologies that surround them.

Lawrence and Lorsch (1967) extended these theories to organisation structures. Their structural contingency theory argues that the governance structure adopted will depend on environmental factors facing the organisation. There will not be one best structure, different arrangements can be equally effective and with evolution, the organisations that can best adapt to their environment will survive.
Lawrence and Lorsch (1967a, p 3) defined the organisation as:

A system of interrelated behaviours of people who are performing a task that has been differentiated into several distinct sub-systems, each one performing a portion of the task, and the efforts of each being integrated to achieve effective performance of that system.

The concepts of differentiation and integration are further outlined in Appendix Seventeen.

The main tenant of the theory can be stated as: “Highly uncertain environments require a high degree of differentiation and integration for effective performance, a state of unstable equilibrium. More certain environments require neither,” Miner (2006, p 229).

Later, this literature review will show that financial institutions are tending to implement separate board risk management committees. The complex and uncertain nature of the banking environment, which leads to complex differentiation and even more difficult integration issues, might be driving this need for a separate board risk management.

Lawrence and Lorsch (1967) used case studies to investigate organisational structures operating in different environments. These studies involved the plastics, foods, container and paper manufacturing industries. A brief summary of these studies is provided in Appendix Seventeen.

One particularly innovative spin-off from contingency theory is the concept of the matrix form of organisation, developed by Davis and Lawrence (1977, 1978) and Lawrence, Kolodny and Davis, (1977).

A matrix organisation is defined as “any organisation that employs a multiple command system with multiple command structures, related support mechanisms and associated organisational behaviour”. In essence, the matrix organisation uses cross functional teams to solve problems.
Matrix organisations come into play, when later in this work, the internal audit, risk management and other governance functions are discussed in the context of integration to develop solutions to governance problems.

Contingency theory has substantial support among scholars of organisational behaviour with an importance rating of 5.39 (Miner, 2006, p 248), but the research has identified problems with the measurement of its major constructs, for example, uncertainty. Nevertheless, the theory has introduced a number of valuable constructs, like the concept of integration, and produced useful developments in the areas of organisational development and for matrix structures.

Carey, Subramaniam and Ching (2006) used contingency theory to study the use of internal audit outsourcing in Australian companies. They found that the size of a firm was related to the extent of outsourcing. Also, small firms, adopting internal audit for the first time, tended to outsource that function. In other words, environmental factors such as the newness of the firm and firm size impacted on the outsourcing decision.

In this study, the use of separate board risk committees, the appointment of CRO’s, and the integration of risk and audit functions was considered. Contingency theory may help explain why some companies adopt one model over another, especially within industry groupings. The complexity of the operating environment may have an impact on the model adopted.

Contingency theory will also help identify why some companies, particularly in the finance industry are setting up separate board risk committees. Is there some environmental factor, differentiation or integration issue in the banking industry that requires a focus on risk management? Once a number of companies head off in this different direction, does institutional theory force other similar companies to follow? These questions help drive the study.
The decision to appoint a CFO rather than a CRO as the head of risk might fall back to an environmental uncertainty issue. Is the volatile banking environment a reason why the CRO position is tending to become the dominant overseer of risk?

The extent of integration between internal audit and risk management might be driven by environmental factors. The maturity of an organisation could be a factor as could the degree to which strategy is important to the success of the organisation. It might be that older, more stable companies in more stable environments tend to adopt the audit profession’s traditional independence model. These questions are explored in the study.

2.3.4 Signalling Theory

Some companies seem to adopt a particular risk management structure as a sign to the market that they are serious about risk management. Signalling theory may explain these actions.

Signalling theory, as discussed by Morris (1987) and Certo (2003), looks at information asymmetry in markets. According to Subramaniam et al. (2009, p9) signalling theory posits that “it would be generally beneficial for organisations to disclose good or improved corporate governance initiatives and practices so as to create a favourable image for the market”. In other words, a company will set up a governance arrangement to flag its commitment to some form of governance to the significant stakeholder market.

Spence (1973) introduced signalling theory to explain how educational qualifications are used as a signal to the labour market, where employers lack detailed information, information asymmetry, on each candidate for a position. Spence outlined the maths behind a basic equilibrium signalling model, and used education to highlight the marginal costs to the signaller, the potential employee, and to the employer.
Liebenberg and Hoyt (2003) used signalling theory to explore the determinants of the implementation of ERM in United States firms between 1997 and 2001. That study involved a control group who had not appointed a CRO matched against group of firms who had appointed a CRO. They investigated whether agency factors such as size, earnings volatility, stock price volatility, leverage, financial opacity, institutional ownership and national location had any correlation to the appointment of a CRO.

Liebenberg and Hoyt (2003) found that CRO’s were concentrated in the energy and finance industries, the theory being that the financial health of these companies is opaque to investors due to financial make-up and a lack of tangible assets.

The appointment of a CRO signals to outside stakeholders, such as S&P and Moody’s, that risk management is important. In this manner, Liebenberg and Hoyt (2003) found that firms appoint CROs to reduce information asymmetry regarding the firms risk profile.

Subramaniam et al (2009, p. 24) used signalling theory to help explain board risk committees in Australian companies. Using a desk-top analysis data was collected from the annual reports of the S&P / ASX 300 Australian companies. Logistic regression was used to define the key characteristics of companies with a risk management committee. They found that when agency costs are high, such as in companies with large boards, risk management is established to signal to stakeholders that the intention of the board is to: “install high quality monitoring mechanisms”.

Certo (2003) used signalling theory to explain how investors use board prestige as a signal of organisational legitimacy. Investors who purchase shares in initial public offerings (IPOs) have limited knowledge of the stewardship behind these previously private companies. This knowledge imbalance between the owner and investor creates information asymmetry.
Certo (2003) showed that this information gap could be reduced by the company adopting a prestigious board structure using high profile individuals with high levels of social capital. This signals the quality of management to investment bankers and analysts.

Morris (1987) outlined the consistencies between agency theory and signalling theory. Both these theoretical frameworks are based on overcoming information asymmetry and both have been used to explain accounting choices, voluntary disclosure and the reasons for the appointment of auditors.


In this study, signalling theory helps to explain what motivates companies to choose different governance systems over risk management. For example, the choice of many financial institutions to use a separate board risk committee might be underpinned by a need to signal a focus on risk management. Similarly, we might find that companies with perceived high risk, such as airlines, food processing and medical suppliers, set up risk mechanisms to highlight their commitment to risk management.

On integration between internal audit and risk management, we might find that some firms chose not to integrate as a governance signal. Such firms will want to signal the independence aspects of a healthy and robust audit function, therefore they choose to keep risk management in a different box.

Finally, the integration between internal audit and risk management may have a theoretical basis. Internal audit and risk management have synergies, a common language and they utilise group problem solving at board level.
The objectives of both risk and audit are to convert expert risk and control decisions into everyday understandable activities that can be embraced by the corporate culture. These similarities are examples of Knowledge Management (KM) and may help explain the synergies.

2.3.5 Knowledge Management

The decisions made on board committees hinge on the knowledge and expertise of independent board members. The choice of key executives is dependent on the ability of those leaders to foster coordination and co-operation. The degree of integration between internal audit and risk management, is underpinned by skills, knowledge and communication abilities. What is needed is a theory that brings knowledge, co-ordination, co-operation, learning and administrative direction into the picture.

At the heart of many theories of the firm is the proposition that a firm can outperform the market. Coase (1952) presented the transaction cost view that directing resources through a firm can in many respects save costs. The absence of costs of negotiating contacts for input materials, when a firm is cooperating with factor producers, is given as an example. Williamson (1991) merges contract law and organisational theory to explain how firms and market behaviour interact.

More recently, there has been a move away from transaction cost economics towards a contemporary theory of strategy. The strategy based theory of the firm concentrates on the benefits of using firms as opposed to the costs of using the market (Connor, 1991, p.132). In this area of study, strategic benefits arise from:
1. resource management (Barney 1986; Rumelt 1984);

2. knowledge management (Connor & Prahalad 1996; Grant 1996);

3. management of key competencies (Foss & Knudsen 1996; Penrose 1959);

4. management of capabilities (Langlois 1992); and

5. real option theory (Barney & Lee 1998; Sanchez 1993).

Item two above, knowledge management (KM), has the potential to predict and explain many of the phenomena observed in this research.

The concept of knowledge as a source of competitive advantage has been evolving in contemporary economics. Toffler (1990) saw knowledge as the “ultimate replacement of other resources”. Reich (1991) contends that, in the future, competitive advantage will reside in those firms “who are equipped with the knowledge to identify, solve and broker new problems”. Quinn (1992) elaborated by stating that most products and services depend primarily on how knowledge based intangibles are developed.

These intangibles include technical know-how, product design, marketing presentation, customer understanding, creativity and innovation. Drucker (1993) outlined a view that knowledge as a resource is now more important than the traditional factors of production, land, labour and capital.

Defining the concept of knowledge has occupied the thoughts of the great philosophers from Plato to Popper. However, there is no clear consensus on the true meaning of knowledge. Knowledge is defined by Nonaka and Takeuchi, (1995, p. 58) as a “justified true belief”. Grant (1996, p 110) defines knowledge, as the tautology, “that which is known”. Liebeskind (1996, p 94), provides a broader definition, “information whose validity has been established through tests of proof”.

38
It is arguable whether a well defined KM theory actually exists, given the lack of consensus on related precepts and purpose. It is however clear that such a theory is currently under development, using the constructs emerging from organisational learning, evolutionary theory, strategic management theory and the resource based view of the firm.

An understanding of the developmental status of KM can be gained from the rationales for why firms exist from the perspectives of the main proponents of KM.

Liebeskind (1996, p 94) argued that firms exist because the firm structure is better than the market at protecting knowledge: “Because property rights in knowledge are weak, firms are able to use an array of organisational arrangements that are not available in markets to protect the value of knowledge”. As an example, Liebeskind (1996) cited employment contracts as a mechanism to hinder external knowledge transfer. These employment contracts include exclusivity, confidentiality and restrictions on competitive behaviour. Deferred compensation plans act in a similar manner. The protection of knowledge gives firms a distinct competitive advantage.

Connor and Prahalad (1996) argued that the competitive advantage of firms comes from the “advantages that administrative direction provides over market contracting”. Market contracts, they argue, need to be renegotiated every time that circumstances change. Employees of the firm, in contrast, can be instructed to change their work practices without the need for contract renegotiation.

Grant (1996, p 112) identifies the integration of knowledge within a firm as a key driver for the existence of the firm:

“Production requires the coordinated efforts of individual specialists who possess many different types of knowledge. Firms exist to create conditions under which multiple individuals can integrate their specialist knowledge”.

39
The integration of knowledge is not straightforward therefore firms that excel at information integration can use that skill for competitive advantage. The difficulty of integrating knowledge can be explained by a number of factors:

1. **Transferability.** Explicit knowledge, or knowing about facts and figures, is knowledge which can be articulated in formal statements, mathematical expressions, specifications and manuals. Such explicit knowledge is easily transferred between parties, almost a public good. On the other hand, tacit knowledge, or know-how, the personal knowledge embedded in individual experience, can only be revealed through its application. The transfer of tacit knowledge between people is therefore “slow, costly and uncertain” (Kogut & Zander, 1992);

2. **Appropriability.** Since tacit knowledge cannot be easily transferred, it is difficult for the firm, or individual, to receive a market return on that resource. Alternatively, explicit knowledge, as a public good, can be resold by any acquirer without losing the good. Also, the making available of explicit knowledge for marketing, often provides that information to potential buyers for free. The difficulties with both transferring knowledge and receiving returns for a valuable knowledge resource, make property rights for knowledge difficult; and

3. **Production.** According to Grant (1996), production requires the coordinated efforts of many specialists who each contribute different types of knowledge. That is not an easy process when the individual specialists will have disparate goals and agendas. Coordination requires rules and directives, planning and routines, group problem solving and decision making.
The major concept behind KM is the premise that firms develop expertise in creating new knowledge and sharing both new and existing knowledge inside the firm. If the firm does that well, it creates a competitive advantage over other firms.

Nonaka and Takeuchi (1995) term this process “organisational knowledge creation” the capability to create new knowledge, disseminate it throughout the organisation and embody it in products, services and systems.

Firms use a number of techniques to facilitate the integration of knowledge. Often these techniques are designed to move between explicit and tacit knowledge or convert one into the other. Grant (1996) summarised these techniques succinctly:

**Rules and Directives**

Probably the lowest cost method of company-wide communications is the written plans, schedules, forecasts, rules, policies and procedures laid down by management. These standards are an attempt to convert tacit knowledge, known by specialists, into explicit knowledge that can be shared across the firm. These company rules are efficient as they minimise communications.

**Sequencing**

Organising production processes into a set sequence allows each specialist to have independent input. Sequencing means that specialist knowledge is integrated while minimising communication. Obviously, the technical characteristics of the product determine the manner in which sequencing can be adopted.

**Routines**

Similar to sequencing, routines are “relatively complex patterns of behaviour, triggered by a small number of initiating signals or choices, functioning as a recognisable unit in an automatic fashion” (Winter, 1986: p165).
Examples such as surgical routines or motor racing pit crew routines show that these learned behaviours can support a high level of reliability and can encompass a wide variety of interactions.

**Group Problem Solving and Decision Making**

Galbraith (1973) pointed out that some tasks will require more personal and communication intensive forms of integration. Meetings, group problem solving sessions and group decision making all involve multiple persons coordinating with one another to transfer tacit knowledge. The need for such highly interactive non-standardised sessions increases with task complexity and with task uncertainty, (Galbraith, 1973). However, this consensus style of decision making is high cost when compared to rules, sequences and routines.

**Common Knowledge**

The integrative techniques discussed above, are often facilitated by an organisational common knowledge. Moreover, it could be possible that the better the system of common knowledge, the greater the competitive advantage.

Common knowledge can be defined as the facets of knowledge that are available to, and known by all organisation members. Grant (1996) suggested that this is aligned with the “intersection of their individual knowledge sets”.

Nonaka and Takeuchi (1995) discussed “information that goes beyond the operational requirements of organisational members, which permits individuals to invade one another’s functional boundaries’ and provides individuals, loosely coupled with each other, a self control mechanism”.

The elements of common knowledge include language, symbolic communication, commonality of specialised knowledge, shared meanings and recognition of individual knowledge domains.
A common language helps knowledge integration where verbal communication is required. This includes rules, directives, problem solving and decision making. Risk Management has a common language, as defined in the ISO 31000 terminology (Purdy, 2010). This allows all those working in risk aware organisations to understand terms such as inherent risk, risk consequence and risk likelihood.

Symbolic communication can include literacy, numeracy, financial awareness, statistics and company jargon that help organisational members acquire organisational knowledge (Grant, 1996). Risk managers understand the concept of a normal probability distribution and the high likelihood of events falling in the 95% probability region.

Commonality is important for information integration. Grant (1996, p. 116) explains that “if two people have identical knowledge, there is no gain from integration. If individuals have entirely separate knowledge bases, then integration cannot occur beyond the most basic level”. The extent of commonality in specialised knowledge drives the level of sophistication of knowledge integration. For example, internal auditors and risk managers are taught the basics of statistics as part of their training processes. This then allows them to share common knowledge at a reasonably sophisticated level, as their knowledge bases overlap.

Shared meanings better allow the conversion of tacit knowledge into a more explicit form. Metaphor and analogy are often used in employee presentations to provide examples of simple known situations that all employees understand.

The analogy of comparing a household budget to a sophisticated corporate plan allows the concepts of increasing revenue, reducing costs and reducing debt to be absorbed by even the least sophisticated employee.
The extent to which each organisational member understands the other individual’s knowledge domain is important for knowledge integration (Grant, 1996, p. 116). Team members can, without explicit communication, work together if they understand the abilities of other team members. This leads to successful coordination and knowledge integration.

Nonaka and Takeuchi, (1995) took the reader through a comprehensive example of how the above rules, routines, common language, metaphor, analogy and group problem solving work in practice. Using the rise of Japanese firms in the 1980’s and 1990’s, they posited that success is underpinned by excellence in knowledge integration.

To outline the conversion of tacit knowledge into explicit knowledge, Nonaka and Takeuchi used the example of the development by Honda Motor Corporation of the Honda City vehicle. Using figurative language, symbolism, creative ambiguity and group problem solving, Honda engineers developed a spherical image, a “Tall Boy” car, tall to maximise comfort and short to minimise engineering. That concept developed into the highly successful Honda City, the company’s distinctive urban car.

KM was useful in this research in a number of areas. Firstly, at board committee level, the combining of financial, risk and audit skills might facilitate the integration of tacit knowledge into the company. Independent directors have strong financial, risk management and internal control skills, all of which require tacit knowledge. Having these directors on a combined board audit and risk committee will lead to stronger knowledge integration at board and senior management levels.

Secondly, the appointment of CROs to oversee both risk and audit functions might also facilitate knowledge integration.
Auditors work with very explicit rules and concepts, often concerning past decisions. Risk managers work with more tacit knowledge, involving subjective future scenarios and possible future outcomes. Independence issues aside, having a CRO over both audit and risk teams, could bring a healthy mix of both explicit and tacit knowledge to that assurance team. The auditors are shown a more subjective view of the future while the risk managers are reminded of the objective nature of internal controls.

Finally, and on a similar theme, the synergy between internal audit and risk management is an often repeated theme in this research. The survey respondents and the interviewees found that the perception of these synergies drives the integration between internal audit and risk management. What the respondents see as synergies is a recognition that common knowledge needs to be managed and shared so that a competitive advantage is created. That integration thus becomes an example of KM.

### 2.3.6 Power Theory

Often, a particular phenomenon can be explained by the political forces behind that outcome or the application of influence or power. This section outlines some of the more influential writers on power theory and how they developed different frameworks for power. The frameworks of power often evolved from the source of that power, examples include knowledge, positional or legitimate, skill, management ability, reward, control of resources, coercion or referent power (Clegg, 1989).

Power was originally defined by Weber (1978) as the ability to carry out a person’s will in a social relationship even if resistance is present. Over time a number of frameworks have developed, each linked back to a particular school of thought on power, (Wickramasinghe, 2006).
The early contrasting views of Hobbes (1962) and Machiavelli (1958) provide a basic grounding in power theory. Hobbes introduced power as being born of legislation, a force that allowed the securing of sovereignty. Machiavelli saw power as a manipulation that could be secured through negotiation, strategies and conflict. Together these writers show that power can be sourced from a number of avenues.

One source of power is the ability to influence and control resources (Dahl, 1957, Lukes, 1974 and Hardy 1996). Resources such as knowledge, information and funding are used to secure desired behaviours, with reward and punishment being the main strategies adopted (Hardy, 1996). Using a budgetary system to direct funding towards a favoured project would be an example of such power.

Another avenue for power is the power of process (Hardy, 1996) previously termed the “Two Faces of Power” by Bachrach and Baratz (1962). Dominant groups use coercion, influence, authority, force and manipulation (Wickramasinghe, 2006, p 343) to secure their objectives. This source of power can also incorporate the withholding of approval, or non-decision which brings a hidden or covert power frame into the argument. The withholding of support by a political party in order to secure support for a favoured initiative would be an example of such power.

Lukes (1974) brings a social dimension into the power frameworks following on from the works of Foucault (1979, 1980 & 1996), a power of meaning (Hardy, 1996). How do structures, rules and agencies influence power? People in organisations follow the status quo and to bring about change requires a sociological input. This aspect of power brings social classes, values and culture into the picture. A church backing a particular political candidate would incorporate a power of meaning.
Clegg’s (1989) circuits of power, or more recently, Hardy’s (1996) power of systems continue the evolution of a theory of power. People follow the status quo, or the systems, cultures, values and beliefs that are tried and true. To change, a break is required, using one or more of the previous powers of meanings, processes or resources.

Power theory and agency theory are intertwined. The preference by agents for short term incentives versus the principles requirement for longer term incentives plays out on a power field. A top of the line CEO may have sufficient expert or referent authority, by virtue of stellar career performance to secure shorter term incentives against the will of the principle.

Institutional theory is also bound together with power theories. Mimetic isomorphism, the copying to seek legitimacy, involves perceived expert power of the organization being copied. Coercive isomorphism is an example of a powerful stakeholder exerting coercion (coercive power) over others. Standard and Poor will downgrade credit ratings for companies that do not adopt sound ERM processes (Meltzer, 2007, p. 48). Normative isomorphism, or peer pressure is a form of expert power. Professional associations and other peer groups possess an expert power reference that enables member companies to follow.

The turf wars that arise when board risk committees come into conflict with board audit committees over jurisdictional matters may result from legitimate power. Each board committee is vying for the legitimate control over risk management matters.

The growing integration between internal audit and risk management may also be a form of power over resources. The requirement to engage with the new risk management discipline can be more easily met if powerful stakeholders, who control resources, utilize the existing internal audit resources.
Allowing the existing internal audit team to become a resource base within the new risk group is a low cost way of meeting a growing regulatory requirement for risk management.

2.3.7 Life-Cycle Model

Using organization life cycle as an explanation for phenomena is more of a framework than a theory. Generally, the life-cycle approach emphasises that all organizations will have different phases of business cycles and will display distinctive behaviours in each stage. The following table summarizes the different approaches to the life-cycle framework. While different writers have different names for each stage, they generally fall into the following matrix (Dibrell, Craig & Hansen, 2011):

<table>
<thead>
<tr>
<th>Age and Size</th>
<th>Birth</th>
<th>Growth</th>
<th>Maturity</th>
<th>Decline</th>
</tr>
</thead>
<tbody>
<tr>
<td>Young and small</td>
<td>Larger</td>
<td>Largest</td>
<td>Declining</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Growth</th>
<th>Inconsistent</th>
<th>Rapid</th>
<th>Slowing</th>
<th>Declining</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication</td>
<td>Face to face</td>
<td>Budgets</td>
<td>5 Year Plan</td>
<td>Poor</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Decisions</th>
<th>Individuals</th>
<th>Teams</th>
<th>Departments</th>
<th>Group think</th>
</tr>
</thead>
<tbody>
<tr>
<td>Competitiveness</td>
<td>Innovator</td>
<td>Competitive</td>
<td>Complacent</td>
<td>Not competitive</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Management</th>
<th>Owners</th>
<th>Professional</th>
<th>Divisional</th>
<th>Politics and conflict</th>
</tr>
</thead>
<tbody>
<tr>
<td>Innovation</td>
<td>High</td>
<td>High</td>
<td>Slower</td>
<td>Resistant</td>
</tr>
<tr>
<td>Profit</td>
<td>Struggle</td>
<td>Increasing</td>
<td>Cash cow</td>
<td>Declining</td>
</tr>
<tr>
<td>Structure</td>
<td>Simple</td>
<td>Developing</td>
<td>Layers</td>
<td>Bureaucracy</td>
</tr>
</tbody>
</table>

Figure 2.1 Characteristics of different stages in the company life-cycle. Adapted from Craig et al (2011)
The birth or entrepreneurial stage (Quinn and Cameron, 1983) is marked by innovation, a struggle to gain customers, small profits and decision making in the hands of the owners. Market penetration has a high focus as does securing funding for ongoing operations. The work-force is diverse and creative with decision making in the hands of the owners. The organizational structure will be simple without the need for boards and board committees.

As companies move into the growth phase (Adizes, 1979) they establish their own competencies (Miller and Friesen, 1984) delegate decision making and start developing management structures. The company becomes more stable (Bonn & Pettigrew, 2009) and decision making starts to centralize (Lester and Parnell, 2008).

In the mature stage (Adizes, 1979) profits are maximized a bureaucracy develops and layers of organizational structure become the norm. Planning and strategy become more prominent, accompanied by policies and procedures. Routines become established and goals become less flexible. Diversity is reduced by the adoption of inflexible rules. There may be decreasing competitive behaviour, complacency and resistance to innovation.

The decline phase is characterized by politics and power conflicts (Mintzberg, 1984) unrealistic optimism and poor communication. Restructuring and retrenchment will surface in an attempt to re-gain former glory (Bonn and Pettigrew, 2009). Profits will decline with loss of market share and control will revert to a powerful few (Lester and Parnell).

The organizational life-cycle framework has been used to study the links between innovation and stage of organizational development (Dibrell, Craig and Hansen, 2011). Auzair and Langfield-Smith (2005) reviewed whether the choice of management control system (MCS) is influenced by the stage of organizational development.
They found that mature and cost leader firms chose a more bureaucratic form of MCS and that organizational life cycle has a significant influence on the choice of MCS.

Having defined the theoretical frameworks, the next sections introduce the emerging debates in the developing discipline of risk management.

2.4 THE DEFINITION OF GOVERNANCE

This section outlines the current debate surrounding the definition of governance. Since both risk management and internal audit form part of corporate governance, the links between governance, organisational structure, risk management and internal audit need to be established. This section also clarifies areas outside the scope of this research.

Colley, Doyle, Logan and Stettinius (2005, p. 5) took us through an agency approach to the birth of publicly owned corporations to explain governance: “Seen as a form of representative government, the owners of these corporations elect directors to govern the business. These directors delegate responsibility to a CEO, set business strategy and oversee results”. All of these activities involve governance.

Probably the simplest view of governance is that put forward by Bosch (1995, p. 7) which portrayed corporate governance as “the systems by which companies are controlled”. The IIA defines governance as “the combination of processes and structures implemented by the board in order to inform, direct, manage and monitor the activities of the organisation towards the achievement of its objectives” (IIA, 2009). These definitions bring organisational systems and structures into the governance framework.

The Organisation for Economic Co-operation and Development (OECD, 2004) brings both relationships and structure into the definition:
“the full set of relationships among a company’s management, its board, its shareholders and other stakeholders, the structure through which the objectives of the company are met”. Clearly risk management forms part of these structures.

In a similar vein, Farrar (2005, p. 3) referred to governance as the control of corporations and the systems of accountability used by those in control.

**Figure 2.2 The structure of corporate governance (Source: Farrar 2005)**

In the above figure Farrar (2005) went further and portrayed a structure for corporate governance which included not only legal control, but also self regulation, best practice and business ethics. Under this view, governance captures a spectrum of interaction and control, ranging from the hard legal reality of corporate legislation, such as the Corporations Act 2001, through to the softer industry and self regulating principles, such as the ASX Principles.

Farrar (2005) extended even further towards the softer cultural aspects and included codes of business ethics and a culture of compliance. Farrar agreed that this model fits with the Keasey, Thompson and Wright (1997, p.2) view that governance included “the entire network of formal and informal relations involving the corporate sector and their consequences for society in general”.

51
Risk management forms part of this governance picture. According to Dickhart (2008, p. 27) the ASX defined governance as “the system by which companies are directed and managed. It influences how the objectives of the company are set and achieved, how risk is monitored and assessed and how performance is optimised”.

In contrast to the above approach, Clarke and Dean (2007, p.61) discussed governance as an outcome, rather than the processes or the mechanics that resulted in that outcome. They argued that governance is really all about accountability and stewardship, concepts that can only be measured by business outcomes or the achievement of objectives. Under this view, tightening the processes that lead to governance will have no effect on the quantum of corporate failure. “None of the mechanisms, either separately or collectively, can overcome the impact of either managerial incompetence or dishonesty, especially at the board level”.

It is difficult to comprehend how governance can be limited to outcomes. Good governance must start before outcomes are reached and involves travelling a pathway. That pathway includes a pre-determined strategic direction, policy parameters within which to travel and controls to prevent straying from the board approved pathway.

Governance is broader than just reaching an objective. Governance must include the pathway and all the processes that steer towards that objective. If the objective is not reached it doesn’t necessarily follow that governance was at fault. If governance is merely the outcome or objective then why not remove boards and let management reign unfettered. Agency theory suggests that unfettered management is unlikely to be in the best interest of the business owner and shareholders.
Sound corporate governance underpins efficient markets and supports growth and economic development. Governance in this context makes good business sense, providing a framework under which investors are more likely to receive economic returns and less likely to suffer from mismanagement, fraud and possible corporate collapse. A number of studies have linked poor corporate governance with questionable financial reporting, manipulation of earnings and even fraud (Beasley, 1996; Beasley, Carcello, Hermanson & Lapides, 2000; Dechow, Sloan & Sweeney, 1996; and Goodwin & Lin Seow, 2002). The link between good governance and financial success was also discussed by Cohen et al (2002) with particular emphasis on the effectiveness of board audit committees and the relationship between poor risk management and corporate failure.

When looking at the reasons for corporate governance, agency theory again becomes relevant. Historically, Berle and Gardiner (1932) identified that the spread of share ownership in American companies had become so great that the owners no longer controlled the companies in which they had invested. They outlined a situation where boards of directors, while legally elected by shareholders to represent their interests, no longer represented those interests and had effectively become “handmaidens for management”, a blurring of the agency relationship between control and ownership.

The agency approach is particularly important when institutional investors are considered. This rapidly growing investment sector, both in number and value, consists primarily of mutual, pension and superannuation funds. These fund managers are now so large and hold such a large percentage of shares in individual companies that they are demanding a say in how their investments are governed.
One example cited by Leblanc and Gillies (2005) is the California Public Employees’ Retirement System (CalPERS), an organisation that takes positions on board appointments and withholds their voting rights on directors if they feel a particular director is not fulfilling proper governance.

Continuing on an agency theory theme, Cohen et al, (2002, p. 579) saw corporate governance as a contractual mechanism designed to monitor management’s behaviour: “the board focuses under the agency perspective are expected to be directed primarily towards monitoring and control, evaluation of corporate performance, global risk management, and management recruiting and compensation”.

Cohen et al (2002) conducted a study aimed at understanding the role of corporate governance in the external audit process. An exploratory, semi structured interview approach was used to question 36 practicing auditors on how they viewed governance in the audit process. The questions included:

1. How do auditors view corporate governance?
2. How is corporate governance viewed in the planning of an audit?
3. Does corporate governance vary across different engagements?
4. How effective is the audit committee versus other governance mechanisms?
5. Has corporate governance changed over time?
6. How will corporate governance change in the future?

For the first question above, Cohen et al (2002) found that corporate governance mechanisms are under the strong influence of management. On the second question, the strength of corporate governance helped underpin the attractiveness of the client. Strong governance mechanisms reduced audit risk and weak boards increased the likelihood of accounting failure.
Cohen et al (2002) also found that governance varied across industries. On the effectiveness of the audit committee, Cohen found that the integrity of senior management was more important than the quality of the audit committee.

The Cohen methodology, using 36 semi-structured interviews, is recognised by the authors as having limitations. “A semi-structured interview approach (e.g. Hirst & Koonce 1996) provides a rich data set, but by its very nature limits the sample size”. Cohen felt that future studies could use supplementary methodologies such as cross-sectional and longitudinal client data or case studies to enhance validity. In this study of S&P/ASX 200 risk management structures, a desk-top analysis and survey will be used to triangulate the interviews and ensure the interview sample is broadly representative of the population.

This debate, which centres on the definition of governance, leads to a research objective that has not been addressed in Australian research. How is the governance or control activity of risk management structured in leading Australian companies?

In this study of risk management structures, the role and influence of the board audit and board risk committees was considered. Also, the roles of the senior executives presiding over these committees, the CEO, CFO, CRO and the CAE were addressed. These governance mechanisms were investigated across a number of agency factors such as industry classifications to see if there are any common practices or groupings.

In this research governance is used in the context of the structures, frameworks and systems that the board of directors and management cast over the ongoing business operations of a corporation. These controls seek to minimise risk exposure which helps the business meet its strategic objectives.
While much has been written about board structure, board composition and board membership, see Green and Gregory (2005), Klein (1998), Beasley (1996), Davidson, Goodwin-Stewart, and Kent (2005), Bathala and Rao (1995) and Lawrence and Stapledon (1999) those specific board related aspects of corporate governance are outside the scope of this study.

The research concentrated on the board committees responsible for risk management, the executive oversight of risk management and the functional arrangements for the delivery of risk management. As the audit committee often presides over, and the internal auditors help deliver, risk management, the relationship between internal audit and risk management is also explored.

The final debate on governance deals with why directors are so interested in the subject of governance. Controversy in that area relates to the extent of liability that can be imposed on directors by the courts.

2.5 THE LIABILITY OF COMPANY DIRECTORS

Governance cannot be discussed without mentioning the debate surrounding the responsibilities of directors. Prima facie, it could be claimed that corporate governance existed purely because it is a good business practice. However, in reality there are other levers at play. Governance systems such as risk management and internal audit are often implemented to signal to society, and in particular to the courts, that directors are meeting their required duty of care. There is a growing tendency for courts to hold directors liable for the actions of the companies which they control. Having solid systems of governance such as risk management and internal audit is a strong mitigating factor in such legal actions.
Austen, Ford and Ramsay (1999) point out company directors face significant penalties if they get corporate governance wrong. In an increasingly litigious society, recent corporate case law is littered with examples of directors who have been prosecuted for failing to live up to their risk management responsibilities. Some of the more noted examples include:

- in the United Kingdom – Barings Bank (Re Barings plc, No 5, 1999, 1 BCLC, 433); and
- in the United States – Enron (Skilling v United States, No 08-1394, 554F, 3d, 529).

The duties required of directors are imposed by both statute and common (general) law. The duties imposed on directors in Canada, the United States, New Zealand and Australia all flow from English common law and as such these duties are reasonably similar.

As outlined succinctly in Baxt (2005), the Corporations Act (2001) sections 180, 181, 182, and 183 impose the following duties on Australian directors:

1. to act in good faith, in the best interests of the company and for a proper purpose;
2. to avoid a conflict of duty and conflict of interest; and
3. to act with care and diligence.

These duties have their roots in the fiduciary duties imposed on trustees who essentially are charged with looking after the interests of others. The meaning of “good faith”, “best interests” and “proper purpose” is determined by reference to previous court decisions which create precedent and provide an interpretation of the law.
When directors fail to meet these duties the penalties are large. Breaches of Sections 180, 181, 182 and 183 of the Corporations Act (2001) carry a maximum penalty of one million dollars and can also result in disqualification from directorships.

Criminal proceedings can also be brought against directors as we have seen in the HIH case and civil penalties can also be imposed. Criminal proceedings can lead to heavy fines and in some cases imprisonment.

Directors are required to act with care, skill and diligence. The care, skill and diligence required of the directors, as interpreted by courts, has grown over time. The decisions in Re City Equitable Fire Insurance (1925) Ch. 407, Commonwealth Bank of Australia v Friedrich (1991) 5 ACSR, 115, and Daniels v AWA Ltd (1995) 13 ACLC 614, show a growing propensity by the courts to require directors to be extremely well informed about the risks that a company faces (Austin et al 1999, p. 322-332). In April 2009 the NSW Supreme Court found seven former non-executive directors of James Hardie Ltd, guilty of breaching their duties and misleading investors. This action centred on a misleading press statement that the board members had failed to read.

Colin Galbraith (2009, p.2), a director of the Commonwealth Bank Australia, stated that the James Hardie decision “emphasised the importance of board fundamentals, such as proper processes, documentation and evidence”. Further he stated that “it is true that it doesn’t just matter what you do, but how you did it and how you show you did it”. Along the same lines, and since the Commonwealth Criminal Code became part of Australian law in 2001, compliance by companies has now become an essential feature of their operations. According to Baxt (2005) a demonstrated culture of compliance will lead to lower penalties being sought by relevant regulators or imposed by the court.
Harrison (1987, p. 111) believed that board committees can assist in limiting the liability of members of the main board: “the use of a board committee tends to limit the liabilities of directors who are not members of a given committee for actions taken by the committee”.

The activities of the board committee will be weighted by the courts when considering whether a company has met an appropriate standard of governance.

If the above view is widely held, there is a strong incentive to create more board committees. Also, a separate board risk committee could effectively shield the main board from unfortunate outcomes resulting from risks that the committee and management agreed to accept. An example would be the fallout from the impact of the United States sub-prime crisis on banks.

These liability questions lead to a research objective aimed at exploring why companies are setting up separate board risk committees and whether such arrangements are particular to specific agency factors. In this study the use of separate board risk committees was investigated. This included the number of companies that use such a mechanism, the industries they are in and the reasons for that choice.

The setting up of corporate governance, risk management and internal audit systems may be merely ceremonial. Meyer and Rowan (1977, p. 343) suggest that rationalised formal structures reflect people’s understanding of social reality. Rules established by the legal system, such as the definitions of negligence, can function as highly rationalised myths that are implemented into organisational structure. For example, a board will set up an audit committee, employ a CRO and set up governance mechanisms to cement legitimacy, thereby reducing the liability of directors. The board will support these activities, regardless of their efficiency.
Modern directors demand sound corporate governance practices and in particular, use internal audit, risk management and compliance systems in order to avoid harsh penalties.

The fact that sound corporate governance is good business sense will be an added bonus. This can be put in context by the words of Baxt (2005, p. 2):

*Risk management and corporate compliance are now central features of the organisation of a company and of compliance by its directors and officers. Failing to ensure that a company complies strictly with laws in these and other areas may have far reaching ramifications for company directors and officers.*

The next section introduces the role of the board audit and risk committees and the emerging debate over their places in modern governance structures. These board committees help directors to carry out and meet the duties discussed above.

### 2.6 BOARD AUDIT OR RISK COMMITTEES

The structure of internal audit and risk management within an organisation was core to this research. Before addressing these agency systems in detail, an understanding of the role of the board committee was required. Board committees provide the top level of governance over risk and audit activities.

In recent years, the oversight of risk management has been delegated by the board to either a board audit committee or a board risk management committee. While the literature shows that the majority of companies use the board audit committee to oversee risk management, there is a growing debate over whether a separate board risk committee is a useful alternative. This section outlines the components of that debate. Exploring which of these models is the preferred practice and why, was an objective of this research.
In line with agency theory, boards set up board committees to distribute the board’s workload and enable more detailed consideration of important matters (Bosch 1995, p17).

The IIA see board committees as “strengthening the role and influence of independent directors” and “providing a forum for improved communication”.

Board committees are advocated in most international jurisdictions. The Combined Code in the United Kingdom, the New York Stock Exchange (NYSE) in the United States and the ASX Principles in Australia, all require robust board committees.

McLellan (2005, p. 67) outlined the most common board committees to be the audit, remuneration and nomination committees. She also added that “a risk committee may be part of the audit committee or may be a separate group, responsible for all areas of risk including operational, environmental, social, legal and financial”.

2.6.1 Board Audit Committee

Boards delegate the oversight of accounting and audit matters to board committees. The most common form of board oversight was provided by the board audit committee and it is normal for that committee to also oversee business risk.

The literature showed that central to the corporate governance functions of internal audit and risk management was the board committee structure. This section outlines the role of the board audit committee.

A Korn/Ferry International (2003) study of 494 Australian listed companies showed that 90%, and 100% of the largest 50 companies, have an audit committee. Audit committees are now legislatively imposed in the United States by SOX and are virtually mandated in Australia by the ASX Principles. The ASX Principles, recommendation number 4.1, states: “The board should establish an audit committee”.
Audit committees evolved from as early as the 1920’s where banks and insurance companies set them up to meet statutory requirements for audits. Burke, Guy and Tatum (2002) provide an excellent chronology of the formation of audit committees over time, interestingly driven by corporate failures.

The financial focus of the board is very important in governance. Reliable and accurate accounts prepared by management and overseen by both internal and external auditors form the backbone of proper governance. These accounts tell the directors how the company is performing against strategic goals, how cash flow and liquidity is managed and they form the basis of both corrective action and follow on strategy. In short, these accounts are the basis for nearly every board decision. Later in this study, it is argued that the annual accounts are, in reality, a score-card underpinning the effectiveness of risk management activities.

The corporate failures of the late twentieth and very early twenty first century provide some strong lessons regarding board audit committees. The Cadbury Report (1992) from the United Kingdom was critical of the ability of executive directors to raise difficult issues with their fellow management team members. In its Code of Best Practice the Cadbury committee recommended the use of audit committees, and to maintain objectivity, the audit committee should comprise at least three non-executive directors.

As a result of recent corporate failures, regulators are now taking a keener interest in audit committees. The following guidelines and recommendations on the make-up and activities of audit committees have been issued over recent years:
1. Institute of Internal Auditors - Position Statement on Accountability and Control, Audit Committees (2001);


3. Sarbanes-Oxley and the New Internal Auditing Rules, Moeller (2004);

4. Improving the Effectiveness of Corporate Audit Committees, 1999 Blue Ribbon Committee of the New York Stock Exchange (NYSE) and the National Association of Security Dealers (NASD); and


The most contemporary view of the audit committee is provided by the IIA publication, noted as point two above. That publication (IIA, 2007, p. 9) outlines the role of the audit committee as including the oversight of:

- risk management and internal control policies and procedures;
- internal and external reporting (financial and non-financial);
- internal and external audit;
- compliance with laws and regulations; and
- the company’s ethical culture.

Since one well utilised model for governance over risk management is through the board audit committee, the role of the audit committee in regard to risk requires a brief examination.
Contemporary literature indicates a shift of focus for audit committees, away from pure financial reporting to holistic risk management. Kloman (2003, p. 1) in his discussion of the changing NYSE listing requirements identified this new role for audit committees, “this work defines a new focus on not only financial reporting but also risk assessment. Risk management is clearly a central challenge for both CEO’s and boards today, along with financial reporting and the audit function itself”.

Crowe Howarth (2010, p. 4) supported a new model for internal audit. This new model firmly advocated a role for risk management in the audit committee. “Seventy percent of audit committee member respondents identified managing risk across the entire organisation as the most challenging near term issue they would face in the following twelve months”.

Board audit committees usually have a charter which details the authority and responsibilities of the committee. Moeller (2004, p. 60) outlines the following responsibilities for an audit committee with respect to risk management:

1. the identification, assessment and management of financial risks and uncertainties; and
2. compliance with legal and regulatory requirements;

While the above relates to the United States context, all of the above points roll risk management and compliance into the purview of the board audit committee. This is a feature of the United States system of governance where internal auditors are also skilled in risk management and compliance.

A KPMG (2005) study revealed that risk is overseen by a board audit committee in approximately 70% of Australian companies. This is supported by Subramaniam et al (2009) who found that in the top 300 ASX listed companies, 75% managed risk through the audit committee.
This study sought to confirm the KPMG and Subramaniam findings and discover the reasons why board audit committees are favoured by the majority of Australian companies.

Finally, audit committees have been in place since the 1920’s. Over time a well established model for structure and operations has been established. Gradually, risk management has been blended into that model and accepted by the key players. From an institutional theory perspective DiMaggio and Powell (1983, p. 148) suggest that: “once a field becomes well established, however, there is an inexorable push towards homogenisation – powerful forces emerge that lead firms to become more similar to one another”.

It seems that, internationally, a strong audit committee, structured around a central risk management theme has taken hold. It would therefore come as no surprise, if that model were to be evident in Australian companies.

Overall, research on the involvement of the audit committee in risk management is scant. While the KPMG (2005) and Subramaniam (2009) studies provide some information, they do not explore the reasons behind the adoption of board audit committees to oversee risk management. In the Australian context, research on the relationship between audit committees and risk is virtually non-existent. Filling this gap in the governance of risk management was an objective of this research. The question that needed to be asked was: “what is the role of Australian board audit committees in risk management and why do such committees become involved in this practice?”

Not all companies structure the governance of risk management through the audit committee. Next we turn to the board risk committee, an area of growing debate, but equally lacking in prior research.
2.6.2 Board Risk Committee

Literature on the question of why some companies are setting up a separate board risk committee and whether that arrangement is particular to specialised industries is scant. That question formed part of this study.

KPMG (2001) defined board risk management committees as:

* a sub-committee of the board of directors that provides enterprise risk management education at board level, establishes buy-in at board level for risk appetite and risk strategy, develops ownership of risk management oversight by the board and reviews risk reports of the enterprise.

In 2009, Subramaniam, Zhang and McManus published on the existence and nature of risk management committees in Australian companies. The motivation for that study was the growth in risk management and the lack of research on the factors associated with such committees: “there is little empirical evidence on factors associated with the existence of risk management committees” (p. 4).

The objectives of that study were twofold. Firstly, agency related factors such as board size, CEO duality, the number of non-executive directors, risk and leverage were examined in the context of whether a risk management committee was present. Secondly, the relationship between these factors and the type of risk committee was examined.

The study drew heavily on agency theory, signalling theory and the drivers arising from the current liabilities imposed on directors in Australian companies. The methodology involved a desk-top analysis of the publicly available annual reports for the top 300 Australian companies using the S&P / ASX 300. A similar approach was adopted in this study, using a desk-top analysis of the S&P/ASX 200 to investigate governance structures.
The Subramaniam et al (2009) study used regression analysis to highlight the relationship between the factors associated with risk management committees. This study will extend the Subramanian study and attempt to explain the reasons why Australian companies are setting up different types of risk management committees.

The study published by Subramaniam, et al (2009) found that, for S&P / ASX 300 companies, 25% had a separate risk committee and 75% combine the risk committee with the audit committee. In that study the researchers found that a separate risk management committee was more likely to be set up by companies having larger boards, higher financial reporting risk and lower organisational complexity. This outcome was further explored in this current study.

The existence of separate board risk committees in the S&P/ASX 200 companies was explored in relation to agency factors.

The ASX Principles, while requiring “a sound system of risk oversight, risk management and internal control”, do not prescribe the specific format. Recommendation 7.1 promotes policies, an internal control system and an internal audit function, but leaves the structure and reporting lines up to the board. A risk management committee is recommended and will be either “the audit committee, a risk management committee or another relevant committee”.

The 2003 Korn / Ferry International study noted earlier found that six percent of the Australian companies studied had a dedicated board risk committee. Also, according to the IIA (2007) publication on good practice audit committees the Australian Prudential Regulation Authority (APRA) now had a requirement for deposit taking institutions to have a board risk committee. That committee however, can be combined with the audit committee. The question that arises from these structures is whether there are any reasons for adopting one model over the other.
The above sections show that companies can structure risk management through either a board audit committee or a board risk committee. Regulators, such as those behind SOX and the ASX Principles appear comfortable with either approach. However, not all parties share such comfort.

Recently, in the United States, a 2009 survey of directors was not supportive of having a separate board risk committee. In that survey, Connelly (2009) reported that 80% of respondents to the Corporate Board Member survey thought that a separate board risk committee was unnecessary. In Connelly’s article, John Deutch (p. 1) commented “As a board we realised that we could not separate risk from audit and do our job. How can you account for assets and set up reserves without assessing risk?” Later in this research, that theme was followed, and is presented as “the synergies between internal audit and risk management”.

An alternative view is offered by the recent Walker Report (2009) into banking failures post global financial crisis (GFC) in the United Kingdom. The Walker Report is based on the premise that, for financial institutions, their core business is the management of risk. Therefore directors of these institutions must take a more active role in, and be aware of, risk management. A finding of that report required that boards of financial institutions have a separate board risk management committee. This may be an example of contingency theory in action, a specific arrangement for a particular environmental circumstance. The Walker Report does however suggest that mandating a separate board risk committee is not without problems:
1. the challenge will be in ensuring a clear separation of responsibilities between the audit committee and the risk committee;

2. with both an audit committee and risk committee in place, the board runs the danger of losing sight of its place in the risk management oversight process; and

3. there is a danger of turning these non-executive director roles into executive ones.

Walker suggested that both committees will “have to work very closely together”. Those themes of “confused accountabilities” are further explored in this study.

Gupta, Watts and Wilcher (2010, p. 19) reported that the Walker recommendation for a separate board risk committee was not adopted for the revised United Kingdom Governance Code (28 May 2010).

Two further recent works shine a different light on the board committee structure debate. Bugalla, Kallman, Lindo and Narvaez (2012) favoured a separate board risk committee. That study used the findings from the Commission into the BP Deepwater Horizon Oil Spill, and the findings from the 2011 Financial Crisis Inquiry Commission, to argue the case for board oversight of ERM. “The failure to have a risk committee at the board level may be an indication of a systemic breach of their fiduciary duty of care”, (Bugalla et al, 2012, p.187).

Bugalla et al (2012) argue that having oversight of risk management through the audit committee creates independence problems. “The board’s failure to have a board level risk committee moves the auditors from their role as monitors of risk to managers of risk”. The author feels that this argument is weak, because internal auditors can monitor the work and outputs from the risk management department without taking on the management of risk.
Most internal auditors currently use a model where they extract specific risk management plans from the risk register and then perform audit work on the adequacy of mitigation measures. That activity in no way places the auditor in a managerial position. At the end of the day, if each individual manager is responsible for risk management, then the ownership of the risk process, location of the risk register and form of ERM is irrelevant. Each manager will use the process to identify risk and allocate resources to manage that risk. The auditor’s role is to check whether enough is being done.

A second study, by Brown, Steen and Foreman (2009) advocated that the complexity of the risks facing the company is the driver for where the governance of risk management should sit. They argued that for low risk companies, they use railroad companies as an example, the board audit committee might be the better mechanism. However, for higher risk, more complex companies, such as biotechnology companies, a management risk committee, comprising subject matter experts, needs to report through to the board audit committee.

Brown, Steen and Foreman (2009) argued that often, in very complex environments, the audit committee members may not have the skills to oversee specific specialized risks. Introducing a management risk committee, with possible audit committee member involvement, brings the subject matter experts into the audit committee envelope.

“A separate risk management committee reporting to the board and the audit committee would be appropriate for many biotechnology companies and companies with a similar level of risk” (Brown et al, 2009, p. 555). In the findings chapter of this thesis, the relationship between the level of risk faced by companies and the risk committee structure adopted is explored in detail.
Separate board risk committees are generally set up by companies that have a core business activity that requires explicit risk management. This may be driven by signalling theory, where for some reason, the company wants to signal a focus on risk management. The National Australia Bank is a good example of this situation. After losing nearly 400 million Australian dollars from a poorly controlled trading unit, the bank was quick to install, and publicise a state of the art risk management function.

Alternatively as noted above, for firms whose business is the management of risk, contingency theory might be behind the choice. Environmental factors such as volatility, uncertainty or even community expectations will underpin the choice of model. Examples would include:

1. credit risk and financial risk management in banks;
2. derivative risk management for traders (i.e. electricity trading and utility companies); and perhaps
3. highly visible risks, such as child care, medical companies, drug and food manufacturers and airlines.

The prominence of risk committees in the banking sector was supported in the Deloitte Financial Services 2004 Global Risk Management Survey which found that:

- Twenty one percent of respondents indicated that risk was owned by a board risk committee; and
- Seventy five percent of respondents from the financial services industry indicated that the CRO reports to the CEO or the board risk management committee.

Goodwin-Stewart and Kent (2006) and Carcello, Hermanson and Raghunandan (2005) both found a relationship between finance companies and the existence of an internal audit function.
The theme of both studies was that finance companies are more risky, are highly regulated and face more compliance risks than other companies. The link between the finance industry and the type of board risk or audit committee will form part of this study.

Subramaniam et al (2009, p.25) found that the size of an organisation is associated with the existence of a risk committee, but size does not correlate with whether that risk committee is separate or part of the board audit committee.

In other words, large companies, with higher agency costs will have a board risk committee, but it could be either combined with the audit committee or a dedicated risk committee.

Risk management cannot be separated from the board audit committee. The audit committee needs to be intimately involved in risk management to focus the internal audit effort and conversely, the internal audit function needs to detect new risks to be reported back to the audit committee for management and mitigation.

There appears to be a significant gap in the Australian literature on the subject of board risk committees. From the population of Australian listed companies there has been very little identification of board committee structures, internal audit and risk management reporting lines and how much integration of these assurance functions is occurring. In addition, the question of whether some Australian companies are managing without a risk management presence at the board level has not yet been asked.

These questions are important as the risk management structure impacts on director liability, costs, business effectiveness and even the signals a company sends to the investment market. The gaps in the literature on the board risk committee make this a fertile area for this research.

It may be that different board risk management structures are aligned with different environmental factors, a contingency theory approach.
For example, smaller companies might tend to integrate internal audit with risk management at board level as an efficiency measure. Larger companies will have sufficient directors to have two separate board committees, an audit committee and a board risk committee.

Bradbury (1990) and Piot (2004) argue that agency related factors such as company size, or more specifically, the number of directors, are positively correlated to the existence of an audit committee. A larger board has the resources to structure board sub-committees from a larger pool of skilled resources.

The issue for smaller companies is whether they can afford to set up board audit, risk and compliance committees and populate such functions with professionals from each discipline. Those questions were explored in this study.

The debate on the role of the board risk committee is central to this research. The structure of risk management at the board committee, executive and operational levels was investigated. Also, the more recent activity of certain specific industries setting up separate board risk committees was examined.

The Chairman of the Australian Institute of Company Directors, Geoff De Lacy, commented in an article in 2005: “the whole area of contemporary corporate governance swings on the complexity of risk and the understanding of risk by the board”. Given this new focus on risk, a question arises over the capacity of the board audit committee to deal with both financial and risk management issues. The next section explores this issue.

2.7 SKILL, TIMING AND WORKLOAD ISSUES

This section examines the current debate over whether the board audit committee can handle both risk and audit matters. This issue is central to understanding how Australian companies structure risk management.
Integrating internal audit and risk management through the board audit committee will lead to skill, timing and committee workload issues. The frequency of board committee meetings and who attends such meetings was raised by the Blue Ribbon Committee (1999) in the aftermath of earlier corporate collapses. These failures also brought to light the level of expertise of committee members.

With the growing complexity of International Financial Reporting Standards (IFRS) and compliance requirements, financial expertise is required on the audit committee.

McMullen and Raghunandan (1996) found in a US study that only six percent of audit committees of financially troubled companies had a qualified Certified Public Accountant on the committee. The Blue Ribbon Committee sponsored by the NYSE and the NASD published recommendations in 1999. These recommendations required that listed companies should have audit committee members with appropriate degrees of financial expertise and financial literacy. In Australia, the ASX Principles have a similar requirement.

In regard to the skill set required to manage risk, Zaman (2001) argued that audit committees lack expertise in risk management and also lack the time to adequately deal with risks. In a similar vein, Spira and Page (2002) found that internal auditors were, in the main, from financial backgrounds and will therefore lack risk management and risk assessment skills. Often internal auditors are seen as having backward looking, compliance skills. Risk managers, on the other hand are required to be forward looking, more strategic people, often working with forecasting models that might be foreign to an auditor.

Increasing the workload of the audit committee by adding risk management, without increasing the number or duration of meetings will lead to inefficiencies.
Alles, Datar and Friedland (2005, p. 122) commented: “audit committee members, however well qualified, often have full time, high level responsibilities elsewhere which inhibit their desire and ability to get more involved with the firm”.

Cohen et al (2002, p. 586), in a study about the role of the audit committee found that external auditors expressed the view that members of the audit committee often lack the expertise to perform their job effectively. “Sometimes members of the audit committee might not be the most appropriate people to be on the audit committee because they lack experience in financial matters”.

In 2007, Fraser and Henry conducted a qualitative study of sixteen audit and risk executives from “Big Four” audit firms and listed companies in the United Kingdom. The study was aimed at examining the ways in which companies identified risks and also investigated how internal audit and audit committees contributed to risk management. A by-product of that research was discussion on the risk management skills held by internal audit staff and audit committee members.

The methodology consisted of free form structured interviews with sixteen participants holding senior positions in listed companies and Big Four audit firms.

The Fraser and Henry (2007) study concluded that:

1. internal audit may lack the expertise to handle risk management; and
2. audit committees lack the time and expertise to oversee risk.

Skill, workload and timing issues are also present in the findings of Harrison (1987) and Alles et al (2005). Both these studies suggested that the increased responsibilities of audit committees, brought on by the oversight of risk management, may be impacting on their ability to function effectively.
One major drawback of the Fraser and Henry study is that the conclusion, the need to set up a separate board risk committee, is based on seventeen interviews. If seventeen different senior managers had been chosen, the results could have been exactly the opposite. This limitation will be taken into account in this current research, where desk-top analysis, surveys and interviews will be used to minimise sample size problems.

The research objective that arises from this debate is, with the added burden of risk management on the board and board committee agenda, how are Australian directors dealing with skill, timing and workload issues?

To the author’s knowledge, there has been no research completed on the skill levels of directors on board risk committees in Australia. Research on whether board audit committees are experiencing timing problems, when the burden of risk management is added, are also lacking. Institutional theory suggests that Australian companies will follow the overseas model that sees the board audit committee used as the central oversight mechanism for risk management. The pressure on director skill levels and the timing of committee meetings, brought on by adding risk management to the financial skills mix, was addressed by this research.

The next section explores the modern concept of ERM an important variable in this research.

### 2.8 ADOPTION OF ERM

Since the purpose of this research is to identify the risk management structures in Australian companies, this section discusses the discipline of risk management in general and in particular the emerging area of ERM. Judging by the amount of literature on the subject, the implementation of ERM by companies internationally is a controversial subject.
This section is required because risk management structures are often established to oversee the implementation of ERM (Kleffner et al. 2003, Liebenberg & Hoyt 2003 and Colquitt, Hoyt & Lee, 1999). Also, the maturity of the ERM culture may drive the adopted risk management structure. Beasley et al. (2005) outlined that maturity to mean the extent of, or progress with, the implementation of ERM.

McNamee and Selim (1998) showed us that productive organisations seek to utilise their assets to create value. This requires interaction between the internal and external environment which creates risk. The management of this risk keeps the organisation viable and productive and as such is part of the governance of the organisation.

Organisations implement governance systems which allow the board and management team to effectively monitor and manage these risks and know that operations are being controlled within defined limits.

In the literature risk is defined by Cooper, Grey, Raymond and Walker (2005, p. 3) as “exposure to the consequences of uncertainty”, by Doherty (2000, p.17) as “the variation in the range of possible outcomes” and by Jorion (2001. p. 3) as the “volatility of unexpected outcomes”. The recently released Organisation for Standards (ISO) standard on risk management, ISO 31000:2009, defines risk simply as “the effect of uncertainty on objectives”.

Dickinson (2001) traced risk management:

as a formal part of the decision making processes within companies from the late 1940’s and early 1950’s, commencing with a focus on insurance products then moving over time to products which managed financial risks.

The two main threads that weave their way through the literature on risk are:
1. Risk has an upside and without risk there would be no reward (DeLoach, 2000, p. xi);
2. Risk has a downside which can be managed. “By showing the world how to understand risk, measure it and weigh its consequences, a group of early thinkers converted risk taking into one of the prime catalysts that drives modern Western society”, (Bernstein, 1998, p1).

The following chart (DeLoach 2000, p. 24) is a useful summary of the evolution of risk management from early insurance and financial risk management towards the modern concept of ERM.

**Figure 2.3 Evolution of risk management**  
*Source: DeLoach (2000)*

As the practice of risk management evolved over time, firms developed expertise in writing insurance, hedging commodity, interest rate and foreign currency risk, leveraging capital structure and dealing with individual project risk. Naturally, and perhaps unfortunately, these risk decisions were made independently, often by different groups or “silos” within a business.
Traditionally, the Finance Department dealt with insurance, Treasury managed derivatives and production engineers managed the risks within projects.

Shapiro and Titman (1986) noted that “because each of these risk decisions affects the total risk of the firm, albeit with different costs and consequences, there are clearly benefits to integrating risk management activities into a single framework”.

In November 2009, the new international standard was adopted by Standards Australia and Standards New Zealand and has been released as Australian/New Zealand Standard Risk Management Principle and Guidelines AS/NZS ISO 31000:2009. This single source international standard, which embodied aspects of AS 4360:2004 and COSO-ERM, allowed risk managers to move forward with a single, united language for risk management.

“Integrated” or “Enterprise” Risk Management entered the scene in the late 1980’s and early 1990’s. Walker, Shenkir and Barton (2003, p. 2) define ERM as “instead of relying on a traditional intra-departmental strategy, ERM adopts a broader perspective that integrates and coordinates risk management across the entire organisation”. A survey of Canadian firms conducted by Kleffner et al (2003, p. 54) resulted in a simple definition: “ERM involves an enterprise wide assessment of risks” and Jorion (2001, p. 472) defined ERM as “aiming to measure, control and manage the overall risk of the institution across all risk categories and business lines”.

ERM has gained importance because of the emphasis now being placed on sound ERM systems by credit rating agencies such as Moody’s and Standard and Poor’s. According to Meltzer (2007, p. 48), “Standard and Poor’s has announced that it will include ERM in its assessment of a company’s financial strength and evaluate ERM practices in its rating of publicly traded organisations”. This means that for most major corporations, deferring ERM adoption is no longer an option.
The importance of S&P ratings might be an example of what Meyer and Rowan (1977, p. 347) discussed as myths that have official legitimacy based legal mandates: “Societies are especially prone to give collective (legal) authority to institutions which legitimate particular organisational structures”. Hence the fact that S&P look for effective implementation of ERM, reinforces the legitimacy of ERM regardless of its effectiveness.

The S&P move to include ERM development in their rating criteria is an example of DiMaggio and Powell’s coercive isomorphism. S&P is a powerful stakeholder within the corporate fabric and can “encourage” organisations to change their structures and practices.

Canadian and United States studies (Kleffner et al 2003 and Liebenberg & Hoyt 2003) show that risk management functions are often established to oversee the implementation of ERM. This work is supported by Gramling and Myers (2006), which used the maturity, discussed further below, of ERM adoption to underpin the role of internal audit in risk management. Therefore, the extent to which each Australian S&P/ASX 200 company has implemented ERM had to be a variable in this study. The level of ERM implementation may drive different risk management structures.

In 2003, Kleffner et al investigated the characteristics associated with the use of ERM, the obstacles preventing adoption and the role corporate governance plays in the decision to adopt ERM. That study used a mail survey to all companies listed as members of the Canadian Risk and Insurance Management Society (CRIMS), followed up by telephone interviews to gain more depth. The Kleffner et al study found:
1. that 31% of the sample had adopted ERM and it was clear that a larger proportion was moving in that direction;

2. the reasons for adopting ERM included: the influence of the risk manager (61%), encouragement from the board (51%) and compliance with the Toronto Stock Exchange (TSE) (37%);

3. the major obstacle to ERM adoption was an organisational structure that discouraged ERM, such as a silo structure, and general resistance to change; and

4. the TSE guidelines were influential in the decision to adopt ERM.

In another Canadian study, Colquitt et al (1999) found that agency theory characteristics, such as industry classification, size, the background of the person responsible for risk management and the placement of risk management within the firm affected the implementation of ERM.

The factors associated with the implementation of ERM in United States companies were also investigated by Beasley (2005) and Miccolis, Hively and Merkley (2001). In the Beasley study a number of agency factors associated with the implementation of ERM were addressed. These included the presence of a CRO, the independence of board members, the support from management, the type of auditor and the organization size, industry and country of origin.

The methodology adopted by Beasley (2005) was an IIA endorsed survey of nearly 1,800 CAEs. A 10% response rate was achieved. The study used correlation analysis to compare the above independent variables against an ordinal dependent variable (ERMSTAGE) which consisted of a five point Likert scale, indicating the extent to which ERM has been implemented. That scale consisted of:
1. No plans exist to implement ERM;
2. Investigating ERM but no decision yet;
3. Planning to implement ERM;
4. Partial ERM in place; and
5. Complete ERM in place.

Effectively this scaling indicates the maturity of the ERM implementation, ranging from no plans, or immature, to completely implemented or mature. A similar style of Likert scale was used in this current study to help understand the extent of adoption or maturity of the ERM process in each S&P/ASX 200 company.

The Beasley (2005) findings indicated a positive relationship between ERM implementation and agency factors such as the presence of a CRO, board independence, management support, presence of a Big Four auditor, entity size and entities in the banking, education and insurance industries.

The implementation of ERM might also be an example of what DiMaggio and Powell (1983, p. 150) term normative isomorphism. Highly regarded regulatory entities such as COSO and the Turnbull Committee have exerted pressure on organisations to upgrade risk management and adopt ERM. Organisations respond by talking to one another, attending industry forums and benchmarking the implementation of ERM. “As a result organisations are increasingly homogeneous within given domains and increasingly organised around rituals of conformity to wider institutions”.

In 2005 KPMG released a survey on the take up of ERM in Australia, which identified a number of issues preventing such implementation. These included:
1. the practice of strategic risk management has yet to be fully integrated into organisations;
2. only half the respondents indicated that their risk management strategy was aligned to business goals;
3. forty six percent of survey respondents did not perform any risk return analysis;
4. only 40% of respondents had developed integrated risk management systems; and
5. the use of technology tools and software had not been widely accepted in driving the risk management process.

All of the above factors are indicators of the maturity of ERM within an organisation. The extent of ERM implementation, or maturity, may underpin the placement and structure of risk management within Australian organisations. As such, the maturity of ERM is a variable in this study.

In this study, the implementation of ERM was investigated as a potential driver to help explain the structure of risk management in Australian companies. In this context, ERM maturity becomes another agency factor like the size of the firm, size and constitution of the board and industry classification. The extent of adoption of ERM may be a driver for how risk management is structured including the arrangements at board level, the integration of internal audit and risk management and the risk management structural models being adopted by Australian companies.

Lam (2003, p. 45) outlines the three major benefits flowing from ERM as, “increased organisational effectiveness, better risk reporting and improved business performance”. Schanfield and Helming (2008), add improved corporate governance to this list of benefits. To gain these benefits a modern risk management system requires a number of attributes. Discussion of these attributes is included in more detail in Appendix Eighteen.
The above discussion indicates that the implementation of ERM is not without problems. To the authors’ knowledge, the extent of such implementation has not yet been measured in research on Australian companies. This research developed a measure for ERM implementation, using a Likert scale, along the lines of the Beasley et al (2005) and Gramling and Myers (2006) studies.

The next section outlines the executive governance over risk management and introduces the role of the CRO.

2.9 EXECUTIVE GOVERNANCE OVER RISK MANAGEMENT

Risk management fits neatly into governance because boards need to know what management is doing to address the risks that face the business. This is one area where agency theory comes into play. Imposing risk management systems and structure is one way of bringing management’s aspirations into line with those of the owners.

This section reviews the literature on the executive structure over risk management. The manner in which risk management was governed at the executive level is a key question in this research.

Australian companies will have different risk regimes, dependent on size, industry sector and other contingencies. Stuart, (2007, p. 21) explains this spread:

At the basic level, there is a risk management policy in place and risk assessment is a discrete, once–a-year activity weighted in favour of consequence and likelihood. At a more mature level, assessment takes place at least quarterly or half yearly. There is also more activity around how risk can be actively managed and moved, either by reducing the likelihood or the severity of the consequences. At the advanced level we see highly regulated entities such as financial institutions. They monitor and measure risk on a daily basis and have clear limits around what can be tolerated.
In 2003, Liebenberg and Hoyt conducted a study that linked the existence of a CRO to the determinants of ERM. The literature review in the Liebenberg study (page 42) provided a sound portrayal of the role of the CRO in the modern organization:

\textit{The CRO will be responsible for identifying, assessing, reporting and supporting the management of worldwide risk issues and opportunities;}

\textit{The creation of the CRO position puts accountability where it belongs, with the leadership team. Risk and opportunity will be measured and managed as a cornerstone of how we do business; and}

\textit{The CRO will be responsible for recognizing and evaluating total corporate risk. That will involve identifying and assessing risks that cut across the organization and then advising the best way to manage them. The new position is necessary for several reasons. Collectively these changes, growth, complexity and innovation, increase the potential for risks aggregating across all operational areas in unexpected ways.}

While overseas literature offered some insight, the literature on the executive control over risk management in Australia was not well developed.

The CRO first appeared in 1993, when James Lam set up an executive position to oversee risk management at GE Capital Ltd in the United States. Dickinson (2000, p. 364) defines the concept of a CRO, as a dedicated ERM specialist, usually a senior executive officer and part of the strategic planning team. Dickinson also discusses the role of the CFO as responsible for the financing of risks, also a senior executive officer and also a part of the strategic planning team.

An international survey of CFO's, CAE's, CRO's and Chief Corporate Counsel's conducted by Tillinghast-Towers Perrin (2001) and sponsored by the IIA Research Foundation found that:
• only 30% of organisations have a CRO as many of the remainder conduct risk management through the CAE; and
• where CRO’s exist, the majority came originally from internal audit backgrounds.

Ernst and Young (2007, p2) highlight the huge diversity in emerging CRO roles: “from a senior actuary in an insurance company to a treasurer with corporate governance oversight”. Ernst and Young (2007) also point to a lack of clarity in the role: “because the risk information required by a construction company is very different to that required by a bank or a manufacturer, their risk management systems and their CRO job descriptions look very different too”. Ernst and Young (2007) felt that, going forward, financially literate, strategically focussed people would fill these CRO positions, and “I wouldn’t be surprised if in five years time, you will be able to study to be a CRO at University”.

The Canadian’s appear to be the leading commentators in the field of executive governance over risk management. Kleffner et al (2003) completed a research project that examined the governance surrounding enterprise risk management in Canadian companies. Their study found that a third of the organisations surveyed had a CRO and that 20% of risk functions reported to the CFO.

In 2003, Liebenberg and Hoyt completed a study on what drives the appointment of a CRO in United States firms. Using the existence of a CRO as an indicator that the firm is adopting ERM, firms with a CRO were regressed against an industry matched control sample. The findings indicated that firms appoint a CRO to reduce information asymmetry around the firms risk profile. Those findings are therefore underpinned by both signalling theory and the Meyer and Rowan (1977) “myth” analogy. Liebenberg and Hoyt (2003) commented that, there was a lack of academic literature on the role of the CRO and on the implementation of ERM.
They also found a lack of consensus on the structure or body that is best suited, within a firm, to manage and implement the ERM program. This study has addressed similar questions in the Australian context.

Liebenberg and Hoyt (2003, p. 32) defined the CRO as, “typically board-level appointees who report directly to a CEO or CFO. These individuals often hold advanced degrees and possess a high level of technical expertise”.

The Deloitte 2004 Global Risk Management Survey, which covered financial services companies, reported that:

- eighty one percent of international financial services companies have a Chief Risk Officer; and
- fifty percent of firms have a centralised risk management approach.

From the Deloitte study it appears that financial services companies will be more likely to adopt the CRO as their senior risk practitioner. The theme of risk management being governed differently in financial institutions, as opposed to other industry sectors, has become a constant in this study. This difference may be due to contingency related factors or from the desire by financial institutions to signal their risk management arrangements to the markets.

Banham (2004, p. 66) when discussing ERM raised the question: “Who should head ERM: the internal audit department – given the new IIA standards – or Chief Risk Officers (CRO’s) and other traditional risk overseers from finance (CFO’s)?” Banham reported that some organisations in the United States are designating internal audit as the better risk manager. The reason given for this is that internal auditors are skilled at setting the benchmarks for internal controls, and as risk management is an internal control, internal audit should therefore be setting the standard for ERM.

Lam (2003, p. 67) stated the opinion that:
Ideally, the day to day responsibility for implementing ERM should rest with an independent risk management function that reports directly to the CEO or board, through the CRO if one has been appointed. This independence ensures that the risk management function is as unbiased and objective as possible.

What is also clear, as outlined by Gambrill 2006, is that to be effective, CROs needed to have a seat at the executive table.

It therefore appears that in some organisations the CFO is the senior executive over risk management while in other organisations the CRO has emerged as the key executive. Indeed, Joe Rizzi, comments in Simkin (2007, p.124) that “the other thing that I would ask for is to try and integrate the CFO functions and CRO functions”. Could it be that the traditionally powerful CFO role is being threatened by the rise of the CRO? And in other organisations could the CAE be taking the lead role in risk management?

The appointment of a CRO, especially in a financial institution signals a strong commitment to risk management. Meyer and Rowan (1977, p. 350) suggest that companies that omit legitimised elements of structure, or create unique structures: “are more vulnerable to claims that they are negligent, irrational or unnecessary”.

A bank that has a strong CRO presiding over risk matters will therefore fare better in the courts and with stakeholders, after some financial crisis. Meyer and Rowan explain this situation using the following quote:

*Failure to incorporate the proper elements of structure is negligent and irrational; the continued flow of support is threatened and internal dissidents are strengthened. The incorporation of structures with high ceremonial value, such as those reflecting the latest expert thinking or those with the most prestige, makes the credit position of an organisation more favourable. Loans, donations or investments are more easily obtained.*
Alternatively, the appointment of CROs by financial institutions might be aligned with DiMaggio and Powell’s (1983, p. 151) mimetic isomorphism. Banks operate in an environment of uncertainty. Their fortunes correlate with economic cycles and, as the recent GFC has revealed, they are not immune from bankruptcy. According to DiMaggio and Powell (1983), uncertainty is a powerful force that encourages imitation. As banks strive for legitimacy they will: “tend to model themselves after similar organisations in their field that they perceive to be more legitimate or successful”.

In a recent article, Caplain (2009) cited three models for the governance of risk management:

1. a consolidated group including governance, risk and compliance;
2. a centralised group under the Chief Risk Officer (CRO); or
3. a decentralised model with a number of different reporting lines.

Caplain (2009, p. 3) stated that all three models have problems, for example the decentralised model only works in very mature organisations that “have the right culture and governance units that are open and cooperative with one another”. The maturity of organisational development, or other such environmental factors, could impact on the risk governance structure.

The lack of knowledge on the executive oversight of risk management is one of the key motivators for this research. To date little research has been conducted on where risk management fits into Australian corporate life. As was found in Canada, is the CFO the lead risk executive in Australian companies or are CRO’s and CAE’s beginning to find a seat on the executive? Will bringing risk experts onto the executive, in addition to the existing financial experts, CFO’s, promote a more strategic flavour to the top management and help balance risk and opportunity?
The next section reviews a potential partner for risk management, the professional discipline of internal audit.

2.10 THE INTEGRATION OF AUDIT AND RISK

Throughout this chapter evidence of the integration of internal audit and risk management has emerged. For example:

1. in the majority, audit committees are overseeing the governance of risk management;
2. the IIA see risk management as a fundamental role of the audit committee;
3. a large proportion of CRO’s come from CAE backgrounds; and
4. the new IIA standards see a strong role for internal audit in risk management.

Obviously such integration has implications for the governance structures over risk management:

- board committees might integrate risk and audit through the board audit committee;
- executive teams might integrate risk and audit under the watchful eye of an experienced CAE or CRO; and
- internal audit teams might integrate with risk management teams at the functional or operational level.

The governance structures over risk management in Australian companies would be difficult to investigate without discussing the role of internal audit. In line with the requirements of SOX, COSO, Turnbull and the ASX Principles, the literature reveals that companies are integrating risk management into the activities of the audit committee. To understand the structure of risk management in Australia, the role of internal audit and its link to risk management needs to be incorporated into this research.
The next section outlines literature which supports the integration between audit and risk management and highlights some possible reasons for integration. That integration will be an evolving paradigm shift.

2.10.1 The Oversight of Internal Audit and Links to Risk Management

Leung, Cooper and Robertson (2004), in Australian research that links internal audit to corporate governance, show that internal auditors perform expert functions in the areas of control evaluation, risk assessment and compliance monitoring, and that corporate governance can be enhanced by further developing these assurance skills.

The IIA (2009) define internal audit as:

*an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and other governance processes.*

Clearly, risk management plays a large role in the internal audit function.

Literature on the manner in which internal audit is governed at the board and executive level is reasonably well developed. The IIA has an international library of information on the role and management of internal audit, concepts fundamental to the existence of that organisation. In 2007, the IIA released a global summary of the Common Body of Knowledge (CBOK), an international study on the profession of internal audit. CBOK 2006 gives a worldwide picture of the demographics of internal audit, the staffing levels across countries, the organisational governance and functional structures, skill levels and competencies of those undertaking these roles.
CBOK 2006 noted an involvement in risk management as the most important emerging role for CAEs. In addition, some of the principal researchers involved in the CBOK 2006, have published separate papers which touch on the governance of internal audit in their region. All these papers highlight the role that internal audit plays in the growing area of risk management (Hass, Abdolmohammadi & Burnaby, 2006, Allegrini, D’Onza, Paape, Melville & Sarens, 2006 and Cooper, Leung & Wong, 2006).

In Australia, Leung et al (2004) published a research project that examined the accountability structures, governance and management relationships of CAEs in Australian organisations. The study found that:

1. fifty six percent of CAE’s reported to the audit committee;
2. forty eight percent of CAE’s strongly agreed that internal audit should bring a systematic and disciplined approach to evaluating and improving the effectiveness of risk management; and
3. seventy four percent of CAE’s see risk management and assessment as the most important aspect of the role.

This new approach blended aspects of internal audit and risk management. In view of this integration, the auditing profession has been searching for the “rules of engagement” that allow internal audit into the risk management space.

Goodwin-Stewart and Kent, (2006) identified the factors that lead listed public companies to create an internal audit function. That paper made an interesting early assumption on page 83, that internal audit is a risk management mechanism. Furthermore, the paper contends that: “internal audit can help organisations identify and evaluate risks, moving the profession into the front line of risk management”.
The Goodwin-Stewart (2006) paper also evaluated several agency theory factors such as commitment to risk management, size and complexity of the company in the decision to build an internal audit function.

Spira and Page (2002) set a milestone for the internal audit and risk management professions. The Turnbull report in the United Kingdom and Treadway (COSO) in the United States both raised the profile of risk management in the governance arena. Indeed, in some respects, risk management became aligned with internal controls and in some aspects even replaced internal control. Spira and Page (2002) sought to shed light on this change to governance thinking, in terms of competition for economic and social resources.

The shift to reinvent internal control as risk management put the internal audit profession head to head with the risk management profession.

Spira and Page (2002) argued that traditionally, internal control is a vague, mutable concept that is difficult to define. This raised a thorny problem for governance practitioners. Regulators, particularly after the corporate crashes of the late 1990’s saw a role for governance in reporting on the internal control environment within an organisation. The internal auditors being the key players in this area gained advancement within organisations from this skill-set. Directors, however, always mindful of litigation argued that a focus on internal controls runs counter to the board’s primary role to foster entrepreneurship and enhance business prosperity.

The redefining of internal control provided a tidy solution to the above dilemma. Shifting the focus from internal control to risk management avoided the problems associated with defining internal control.

Also changing internal control to risk management overcame the problem of using internal control as an entrepreneurial blocking argument. Risk brought in a positive side which underpins organisational success.
The redefinition of internal control as risk management meant that UK companies could now rely on assessing their risk systems rather than the former internal controls. External auditors are now marketing their risk services and risk advisory practices are becoming commonplace. Specialist risk management consultants are appearing, offering advice on Turnbull implementation.

Spira and Page (2002) discussed the opportunities for internal audit from this metamorphosis. Traditionally, internal auditors fulfilled compliance and monitoring roles as: “organisational policeman and watchdog” (Morgan, 1979, p. 161). More recently, the IIA has redefined internal audit to encompass more risk management and consulting involvement: “independence and objectivity, identifying an assurance and consulting role for internal audit and emphasising adding value and improving effectiveness of risk management” (Spira and Page, 2002, p. 653).

Internal auditors have been quick to portray themselves as risk management experts, based on their association with internal controls. However, the effectiveness of internal auditors in the risk management sphere is not obvious. Survey work by Griffiths (1999), found negative attitudes to internal audit, being: “too low key and basic, insufficiently business oriented and lacking in skills and properly trained staff”.

The redefinition of internal control as risk management and the quest for internal auditors to move into that space is a fundamental construct in this study. The Spira and Page (2002) work sets the context for the role of risk management within organisations and the role of internal audit within risk management.

Both the structure of risk management within S&P/ASX 200 companies and the levels of integration between internal audit and risk management may be dependent on this redefinition of internal controls to risk management.
The level of integration, the impact of audit independence and even the effect on internal audit outsourcing are all affected by this paradigm shift. Those issues are all objectives considered in this study. The question asked by Blackburn (1999, p. 6): “which should come first, risk or control” is addressed in this study by asking whether internal audit is a sub-set of risk management.

The literature on the oversight of internal audit is reasonably well developed. There is however, a lack of research on how the integration of internal audit with risk management is impacting on governance structures. This study investigated the relationships between risk management and internal audit and how such relationships are handled at the board, executive and functional levels within Australian companies.

The next section discusses an evolution of the nexus between internal audit and risk management.

2.10.2 An Emerging Paradigm Shift

Internal audit has changed dramatically over time and may be experiencing a further shift which involves the integration with risk management. In Figure 2.4, McNamee and Selim (1998) identify the passing of two major internal audit paradigm shifts. In the initial paradigm the role of internal audit in corporate governance, pre-1940, was aimed at re-performance or observation and counting. Moeller (2005) portrays this initial paradigm as internal auditors being little more than in house assistants for the appointed external audit firms.
During and coming out of the war years, the accepted father of modern internal audit, Victor Brink, (Brink, 1942) introduced the first paradigm shift. He revolutionised the discipline by advocating a new focus on internal controls and installing internal audit as a valued service provider to management.

In more recent times a second paradigm shift has emerged. McNamee and Selim (1998, p. 1) see this new paradigm as allowing risk management to underpin the auditing profession: “both internal auditing and risk management are co-evolving with the ascendance of global business risk as a major corporate governance issue”.

This new paradigm recognises: “that risk is the driver of organisational activity and corporate governance is the organisation’s strategic response to risk”.

It appears from the literature that internal audit is embracing this next paradigm shift and is moving towards a risk based approach. This is best summarised by the following table which contrasts the earlier control framework to the now universally adopted modern risk based framework for internal audit.
### Characteristics

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>Old Paradigm</th>
<th>New Paradigm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Audit Focus</td>
<td>Internal Control</td>
<td>Business Risk</td>
</tr>
<tr>
<td>Internal Audit Response</td>
<td>Reactive, after the fact, discontinuous, observers of strategic planning initiatives</td>
<td>Proactive, real-time, continuous monitoring, participant in strategic plans</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>Risk Factors</td>
<td>Scenario Planning</td>
</tr>
<tr>
<td>Internal Audit Tests</td>
<td>Important Controls</td>
<td>Important Risks</td>
</tr>
<tr>
<td>Internal Audit Methods</td>
<td>Emphasis on the Completeness of Detail Controls Testing</td>
<td>Emphasis on the Significance of Broad Business Risks Covered</td>
</tr>
<tr>
<td>Internal Audit Recommendations</td>
<td>Internal Control: Strengthened Cost Benefit Efficient / Effective</td>
<td>Risk Management: Avoid / Diversify Risk Share / Transfer Risk Control / Accept Risk</td>
</tr>
<tr>
<td>Internal Audit Reports</td>
<td>Addressing the Functional Controls</td>
<td>Addressing the Process Risks</td>
</tr>
<tr>
<td>Internal Audit Role in the Organisation</td>
<td>Independent Appraisal Function</td>
<td>Integrated Risk Management and Corporate Governance</td>
</tr>
</tbody>
</table>

**Figure 2.5 Old versus new internal audit paradigms: Source: McNamee and Selim 1998**

Birkett, Barbera, Leithhead, Lower and Roebuck (1997) identified that this new paradigm would require: “a set of new competencies for the internal auditing profession, a new language for risk and a broadening of the role of the CAE”.

This new risk paradigm involved internal audit using the products of risk management, but fell short of full integration between the internal audit and risk management functions.
The above table shows another important change in dimension. In the old, re-performance paradigm the internal audit role was backward looking and compliance oriented.

This made the audit role a non-strategic, almost “policeman like” type of role. These early less mature organisations lacked trust and needed the auditor to check on the integrity of employees. Auditors demanded independence and would not participate in executive management teams. This created a tension between management and the auditors, who were seen as: “looking over management’s shoulders”. Management saw little value in this policeman like role.

The shift to base internal auditing on risk will be just the tip of the change. It seems that an extension to the third or perhaps even a fourth paradigm is beginning to emerge. As can be seen in Figure 2.6, this next paradigm sees internal audit, risk management and perhaps even compliance and ethics being swept into a single bucket driven by the significant corporate failures in the 1990’s and early 2000’s and reinforced by the current GFC.

Under this new approach the auditor looks to the future, rather than concentrating on the past. Focusing on current risks moves the auditor into a world where present transactions and future transactions become more important. This overcomes the backward looking theme of traditional internal audit, a theme that has prevented management from seeing the true value-add from the audit function.

Selim and McNamee (1999, p. 170) support this next extension to internal auditing while developing a model for the risk management and internal audit relationship. They see: “the value of a strong relationship between risk management and internal auditing with – internal audit being the other side of risk management”.

98
Under this new approach, internal audit works in partnership with management, identifying strategic risks and ensuring that mitigations are helping to manage those risks. Independence becomes less of an issue in a model where maturity, integrity and collaboration replace the policeman like reliance on compliance. With internal audit and management in partnership, management can start to value the strategic contribution of the auditors.

Evidence of this third paradigm shift has recently been supported by Ernst and Young (2009) which showed that the credit crunch aftershocks and the deepening global recession have displaced regulation and compliance as the top risks facing international companies. Ernst and Young report that, as a response, internal audit functions are repositioning and re-tooling to cover assurance over strategic risks and business performance targets.

Ernst and Young (2009, p.1) advocate that the integration of internal audit with ERM is an important first step in the transformation that “broadens internal audit’s focus to include strategic and operational risk as well as business improvement”.

Figure 2.6  The next paradigm shift. Based on McNamee and Selim 1998 (an extension of Figure 2.4)
Even more recently, Chambers (2009) talks about the GFC as encouraging a move by internal audit to the next paradigm. With respect to a changing internal audit model, Chambers (p. 28) notes that:

*This paradigm now requires an updated scope and delivery method to meet future needs. The next shift is likely to offer overall assurance to the board, and even to external stakeholders, on the identification and mitigation of both internal and external risks.*

The synergies between internal audit and risk management will be driving this third paradigm shift, a fuller integration of the two disciplines. In Australia, where companies are generally smaller and where the ASX Principles do not fully mandate an internal audit function, full integration makes economic sense. This study investigated whether such a paradigm shift is occurring in Australian companies. Establishing the level of integration between internal audit and risk management in Australian companies was a major objective of this research.

The next section outlines the synergies between internal audit and risk management. Integration will be a natural consequence of such synergy.

### 2.11 THE SYNERGIES BETWEEN AUDIT AND RISK

This section discusses the common threads between the governance functions of internal audit and risk management. If these disciplines have sufficient overlap and commonality, there is an argument for integration. To date, nothing has been published on the synergies between internal audit and risk management. Yet board audit committees are embracing risk management, and CRO’s are beginning to preside over internal audit functions.
Traditionally the functions of risk management and internal control were part of the job description for every manager. Twenty years ago, perhaps even ten years ago, the existence of a professional risk manager was very rare indeed. Each senior manager was expected to keep abreast of the limited number of regulations applying to his or her profession. Risk management was all about looking forward and anticipating obstacles which needed to be managed to achieve objectives. The first line of defence for boards was the employment of experienced managers who undertook risk management as part of their daily activities. This is still the case. However pressure from recent corporate collapses, the growing levels of regulation and a clear view by the courts that documented governance systems help in actions against directors have all contributed to a requirement for more explicit risk frameworks and risk management systems.

When looking at corporate governance, regulators in the United States, United Kingdom, Australia and Canada have all identified the agency controls of compliance, risk management and internal audit as fundamental building blocks of corporate governance. This can be most clearly seen in the ASX Principles, which require an audit committee, and sound systems for risk management and compliance. This fundamental building block view hinges on the concept that risk management and internal audit are both systems within corporate governance or systems of internal control. If viewed in this manner the concept of integration makes good sense.

PricewaterhouseCoopers (PWC) (2007) completed a survey of internal audit executives in United States corporations. They found that nearly one third of the internal audit teams surveyed were responsible for the ERM function within their organisation. Also the PWC survey found that there is growing recognition of the strong link between effective risk assessments and effective audit coverage.

It is clear that the disciplines of internal audit and risk management have substantial overlap. The following sections highlight these synergies under the headings of:
1. management responsibility – both internal audit and risk management help facilitate a management responsibility;

2. functional objectives – of risk management, internal audit and compliance, are all aimed at risk management;

3. control systems – both risk management and internal audit are systems of internal control;

4. three lines of defence – the synergies in action; and

5. efficiency and effectiveness – given the synergies, can companies afford to separate the functions?

2.11.1 Management Responsibility

Management responsibility in respect of each of these functions, has a common thread. Both internal audit and the centralised risk management unit provide a checking, guidance and facilitation role for management who maintain the primary accountability for the activity.

Internal audit is not responsible for internal controls, management has that responsibility. SOX (2002) required an internal control report that “affirms the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting”.

The risk management function is not responsible for identifying and mitigating all risk, again, management has that responsibility. According to McNamee (1997, p4) the risk manager “acts as a catalyst and a resource for extending the thinking processes of the management team, a teacher, who operates closely with other managers in ad hoc teams to improve the organisation’s business processes”.

The two functions have an underlying objective to support management in achieving management’s responsibility to have adequate internal controls, sound risk management and systems to comply with laws. This support requires administration of software systems, identification of champions, consulting on technical aspects, assistance with cultural change and reporting back to the board, or board committees, on the integrity of these control systems. To this extent, internal audit and risk management overlap.

2.11.2 Functional Objectives

When looking at the objectives of the professional disciplines, as offered by their associations in Australia, we see substantial overlap:

1. The Risk Management Institution of Australasia Ltd (RMIA) website (2006) has the mission to “champion the concept of risk management as a legitimate business discipline in its own right”.

2. The key objective of the IIA (2006), according to their website, includes: “to provide leadership on the standards and practices of internal auditing, including risk management, internal control and governance”.

3. The Australian Compliance Institute (ACI) website: “advocates a holistic approach where compliance, ethics, governance and risk management are managed as interconnected disciplines that add to the integrity and trust of an organisation”.

Both the internal auditors and compliance managers see risk as a fundamental component of their domains. The risk managers, not wanting to be absorbed into audit or compliance, seek a separate status.
In October 2008, Mark Phillips (p. 15) interviewed Grant Whitehorn, president of the RMIA, on collaboration between the professional risk management bodies noted above. In that interview Whitehorn explained that all three bodies were trying to facilitate risk management to build resilient organisations. However, because of the politics behind the organisations, each was trying create individual standards based on their own discipline.

As discussed above risk management and internal audit are both part of governance. Are these processes both systems of internal control?

### 2.11.3 Systems of Internal Control

Internal audit and risk management are both systems of internal control. Internal audit allows the audit committee to understand the systems of control that management has placed over day to day operations. Risk management allows the audit committee to understand the main risks identified by management and what mitigating controls are being implemented. Under this view, it makes sense for both operations, internal audit and risk management, to move closer together.

The merging of internal audit with risk management is a theme identified by Spira and Page (2002). That study took the reader through the growing influence of risk management in COSO, CoCo and the United Kingdom Combined Code. The paper finished on the more recent Turnbull recommendations (p. 650) which: “couple internal control with risk management throughout”.

Spira and Page (2002) indicated that adopting a role in risk management is an opportunity for those seeking to professionalise the internal audit profession. On page 654, they note: “Internal auditors, traditionally specialists in internal control but not highly regarded within organisations, have attracted the attention of boards grappling with external demands for assurance about corporate governance practice”.
The IIA shift to allow consulting is seen as positive as is the move to outsourcing, where Big Four internal audit firms are more closely aligned to risk management. Deloitte (2000, p.6) summarised this aspect:

*The shift in the risk control landscape creates both challenges and opportunities for internal auditors. Those that handle the challenge quickly and cost-effectively will be credited with helping their organisation meet its business goals. Those that don't will be left behind stranded in a world where the attitude “you are either part of the problem or part of the solution” separates the survivors from the casualties. There is still much work to be done and we hope that the internal audit professionals will see beyond today and carve a vision worthy of tomorrow.*

Earlier, governance was defined, in one context, as the systems for organisational control. Directors are exposed to an onerous duty of care and need to show or signal that they and management have implemented appropriate systems for controlling company direction. These systems include identification and mitigation of risk, controls related to financial accountability and compliance with policy and law. These are all systems of internal control that are designed to manage risk.

2.11.4 **Three Lines of Defence**

The financial services sector is embracing the synergies between internal audit and risk management. The three lines of defence model first came to prominence in 2006, when it was explained in the annual report for the National Australia Bank under Risk Management – Introduction, page 15. The model is gaining favour in the financial services industry.

The model uses three lines of defence to manage risk, blending management, the risk system and internal audit. Micallef (2008) explained these three lines as:
1. The first line of defence is the board, CEO, senior and operational management. The board set the risk strategy, the CEO takes responsibility and line managers actually manage the risks, using a chosen ERM framework;

2. The CRO, and the risk function, is the second line of defence. That team recommends risk policies, oversees the ERM system and provides guidance to management;

3. Finally, internal and external audit provide assurance on the first two lines of defence.

The three lines of defence model is a practical example of the integration between internal audit and risk management. While each is a separate discipline, they merge as a barrier to prevent risks from destroying corporate value.

2.11.5 Efficiency and Effectiveness

Finally, with the increasing costs of doing business, brought on by more regulation and the growing liabilities for directors, efficiency and effectiveness become important. For a smaller company it seems inefficient to have a head of audit (CAE), head of risk (CRO) and perhaps even a head of compliance. Mike Lotzof (undated, p. 3) the CEO of the ACI put forward a view: “typically, compliance, ethics, governance and risk are treated as separate silos that sit ponderously above and separate from the organisation’s business objectives, systems and processes. This is inefficient and ineffective”.

The disciplines of internal audit, risk management, and compliance overlap. All are aimed at managing risk, all require knowledge of risk management, all are internal controls and all require an understanding of corporate governance. In addition, they all provide support to management and directors, assisting them to meet their internal control responsibilities, duties and obligations.
This research sought practical models for risk management in leading Australian companies. These models will see the assurance disciplines converge together as is largely the practice overseas.

This convergence was identified by KPMG (2005) and Subramaniam et al (2009) earlier, without attempting to uncover the reasons. The similarities between internal audit and risk management, discussed earlier, indicate that integration would be a natural outcome. The overseas experience confirms a trend towards integration. There is however, a significant barrier that might prevent such integration.

2.12 BARRIERS TO INTEGRATION

This section considers the major barrier to the integration of internal audit and risk management, the underlying concept of internal audit independence. The discussion covers:

1. the impact of auditor independence;

2. whether such independence is real or illusionary; and

3. the role for internal audit in risk management.

2.12.1 Auditor Independence

In the view of the IIA, internal auditors cannot be fully responsible for ERM because this would create a major conflict of interest when the internal auditors come to audit and attest to the ERM systems and processes.

All internal auditors who are members of the IIA are required to conform to the International Standards for the Professional Practice of Internal Auditing (2009). Section 1100 of the IIA standards requires that: “the internal audit activity must be independent, and internal auditors must be objective in performing their work”. Independence is impaired where the internal auditor has a conflict of interest.
Technically this means that internal auditors cannot be involved in the risk management process, make decisions about that process and then undertake an audit of a process with which they have been intimately involved.

The concept of independence is the essence of internal auditing. Indeed the concept of independence to some auditors is likened to the importance of the Hippocratic Oath to a doctor of medicine (Christopher et al, 2009). To others, this dogmatic insistence on independence is a drawback preventing change and could eventually challenge the relevance of the internal audit profession.

To illustrate this contrast on independence Arena and Azzone (2005, p. 12) carried out a case study in Italy aimed at reviewing the relationship between internal audit and risk management functions. They found a wide divergence on how internal audit interacts with risk management. The involvement of internal auditors ranged from: “assurance over the ERM process, to support for ERM implementation, to complete management of the ERM process”. This spread of involvement centred on how strongly the organisation viewed auditor independence.

Signalling and agency theory will be present when audit independence is considered. A company will, for agency reasons, want to assure the principal, the shareholders, that a strong internal audit monitoring function was cast over the agent, management. An independence breakdown, or having the agent too close to the auditor, would be problematic. The company will signal its commitment to a strong internal audit function by emphasising the independence element of that governance function.

The supporters of strict independence, arguably the more traditional internal auditors, avoid involvement in management decision making so that they cannot be compromised and can later audit the results of those management decisions.
These auditors therefore, are reluctant to become involved in risk management functions or indeed to become members of the top executive team. This attitude can also drive the internal audit function down into an intermediate position in the organisational hierarchy, where, even if independent, the internal auditor becomes ineffective.

The IIA has recognised that the independence requirement will inhibit the internal audit involvement in risk management. To overcome the problems with independence, the auditing profession has created a set of rules regarding internal audit involvement in risk management. These rules are based on management retaining responsibility for ERM and internal audit providing underlying support and assurance. This aligns with the traditional role of internal auditors, to audit and attest to the internal control systems for which management is responsible.

The following chart outlines the areas of demarcation between internal audit and enterprise risk management as portrayed by the IIA, England and Ireland (2004).

![Figure 2.7 Internal audit and ERM](image)

*Figure 2.7 Internal audit and ERM*  
*Source: IIA (2004)*
Figure 2.7 breaks ERM into three segments:

1. core roles that internal auditors should be involved in, e.g. evaluating risk management processes;
2. roles that internal audit can get involved in with safeguards to ensure independence, i.e. training management in responding to risks; and
3. areas that internal audit cannot undertake, e.g. being accountable for risk management.

Matyjewicz and D’Arcangelo (2004, p.1) fleshed this model out by stating that: “internal audit can play a key role in ERM, providing assurance on ERM policies and procedures, without compromising auditor’s independence and objectivity”.

Therefore, the IIA standards as supported by leading commentators do allow internal audit into the risk management space, provided safeguards are adopted. The independence issue does however set up a barrier to a clean integration of internal audit and risk management. The next section argues that the entrenched dogma of independence may not be as big an issue as it is often portrayed.

The above section reinforced the strength of independence as a driver for the internal audit profession. However delving into more detail exposes some cracks in the concept of independence. These cracks are part of an ongoing debate in the profession.

2.12.2 Is Auditor Independence an Illusion?

The requirement for internal auditors to remain independent has practical problems. Christopher, Leung and Sarens (2009) identified the tension that currently exists within internal audit functions regarding independence. On one hand these functions strive to be accepted by providing management with value-adding services. On the other hand they are required to provide independent advice to the board.
The Christopher et al (2009) study used a survey instrument to gain insight into whether internal audit functions operating in this tense environment are really operating independently. The study was underpinned by both agency and institutional theory. Agency theory explained the actual existence of internal audit functions. Their responsibility was to provide independent advice to the principal, the board or audit committee, regarding the performance of the agent, management. Institutional theory was also used in the context that internal auditors need to report to the agent in a manner consistent with social expectations.

Two of the objectives of the Christopher et al (2009) study were important for this current study. Both objectives relate to internal audit independence:

1. to what extent is the internal audit function independent from management? and

2. does the relationship between internal audit and the audit committee provide for independence?

An email survey instrument was used for the Christopher et al (2009) study because it allowed large scale data gathering with decreasing costs as the sample size increased. The IIA sponsored the survey, adding legitimacy, and forwarded it to their list of 206 Chief Audit Executives. Thirty four responses were received giving a response rate of 17%.

The study found that all internal audit functions surveyed were placed at the appropriate group level to support independence. In other words, they were not intermediate level functions, but were well placed in the hierarchy. However, the majority of respondents identified that internal audit is a “training ground or jumping stone” (Christopher et al, 2009, p. 15) for promising staff to move on to management positions. This raised a potential problem for independence:
“can internal auditors raise reports against management, independently, when they are dependent on management for a career in a future operational role”.

The study found that in 30% of cases, either the CEO or CFO approved the internal audit budget. The study also found that in 64% of cases, the CEO and CFO had a strong influence on audit planning. When added to the potential for management to control the career paths of auditors, the budget approval and audit planning influences could compromise independence. This outcome is consistent with the Cohen et al (2002) finding that corporate governance mechanisms are often strongly influenced by management.

Finally and most importantly for this current study, the study indicated that 56% of internal audit functions perceived internal audit to be a partner to management. Christopher et al (2009, p. 16) argued that: “this culture may indirectly put additional pressure on internal audit to work with management to achieve a common goal rather than act as a separate independent body checking on them”.

The results of the Christopher et al (2009) study are important for this current study. Firstly, combining risk and audit responsibilities at the audit committee level will impact on auditor independence. Second, integrating internal audit and risk management functions makes internal audit more likely to become a partner with management. This could compromise independence in the Christopher et al paradigm.

The benefits of a collaborative, partnership approach might outweigh the traditional independence view. This is particularly the case in a modern internal audit world where compliance auditing is being replaced by collaborative risk management and problem solving. “The internal audit function has evolved from corporate cop to that of a savvy in-house consulting service”, Christopher McRostie (2008) CEO of IIA Australia.
The survey methodology used by Christopher was interesting, in that it only achieved a 17% response rate, which is low enough to raise questions about the results and create bias. This current study used a mail based survey approach, strictly adopting the Dillman (2007) methodology for enhancing response rates. In the current study, the author aimed to achieve a response rate approaching 50%, thereby reducing accuracy, bias and reliability concerns.

The IIA also allows internal auditors to take on a consulting role. In such a role, the auditors advise management on steps to improve process or tighten internal controls.

Such advice on improvements is allowed under the IIA rules, as management retain responsibility for the improvement and can reject the audit recommendation if they so chose. If management adopts the recommendation, they, not the auditors will implement the change. The IIA may have, through the consulting role, conveniently given internal auditors a way to by-pass the independence issue. There is debate however, over where the internal audit role ceases and where the consulting role begins.

A recent survey conducted by Protiviti and the IIA Australia (2009) supports the illusionary nature of auditor independence. That research found that:

1. a significant number of internal audit functions lack the appropriate framework to operate independently and objectively;
2. an excessive level of influence is exercised by executive management over the audit committee; and
3. the majority of internal audit functions are unable to demonstrate compliance with International Standards on the independence issue.

As a result of these practical limitations on independence, and more in line with the consulting role, a “partnership” concept as discussed by Eisler and Loye (1998), has emerged.
The partnership approach sees auditors working with management as team members, to achieve a common goal rather than acting as a separate independent body checking on them. This move goes against the traditional views on independence and objectivity. Christopher et al (2009), as noted earlier, see this working with management to achieve a common goal as a threat to independence. However, this partnership approach has merit and will be part of the paradigm shift discussed earlier, bringing risk management and internal audit closer together.

The traditional role of internal audit, we have seen, concentrated on internal financial controls. This was a backward looking model, directed towards the assurance of compliance with policy and procedure. This policeman style of role reviewed past events, was non-strategic and was not seen as adding any value by management (Spira and Page, 2002, p. 655, Christopher et al, 2009, p.6). Turner (2009, p.6), quoted Christopher McRostie, the CEO of the IIA in Australia:

*In rapidly changing and increasingly complex business and regulatory environments the internal audit function has evolved from corporate cop to that of a savvy in-house consulting service, that not only reports problems, but that also gives constructive suggestions to line managers about how to improve the performance of the business.*

This aligns with the IIA’s (GAIN, 2009, p. 3) statement on the GFC: “A shift in stakeholder expectations is requiring that internal auditors take on a more strategic role, with risk management activities taking precedence over other controls and compliance auditing”. The modern internal auditor is trying to break free of that backward looking mould. Nowadays internal auditors see themselves as having a strategic focus, with a view to the future and with a breadth of audit coverage that adds value to the management team. They see themselves as valued consultants.
At another level, the trend for CAE’s to report to a board committee, rather than to an executive management position will assist in maintaining independence. Ernst and Young conduct annual surveys of the reporting arrangements for CAE’s in Australia and New Zealand. These surveys show a growing trend for CAE’s to report through to the chair of the audit committee. This reporting line helps establish a partnership approach with management. Internal auditors can work more closely with management, unfettered by independence issues, safe in the knowledge that they can report to the audit committee if management raise barriers or try to block the internal auditors.

As organisations mature, the need for integrity overtakes the need for independence. In a mature organisation, management welcomes internal audit as a valued part of executive management, a partner contributing expertise to help reach the company goals. Management sees the auditor as a valued partner and allows the auditor access to information and takes audit comments seriously, whether they are negative or positive. In a mature organisation, management do not fear retribution when an auditor finds a problem. The organisation views the finding, communication and solving of such a problem as a “good” and rewards such behaviour. Maturity and integrity become partners, taking over from independence. As noted earlier, Caplain (2009) sees the organisation's culture and level of maturity as fundamental to the risk management structure. Governance units that are open and cooperative with one another will have outgrown the need for overt independence.

Christopher et al (2009) suggest that mature organisations might develop strategies that allow the internal auditor to engage in consulting, not decision making, activities without compromising independence. These strategies include reporting to the audit committee and holding private meetings with the audit committee chair. Parkinson (2009), writing on the “assurance versus consulting debate” supports this argument.
He adds that internal auditors can develop mechanisms that reduce the impact of consulting advice on independence and objectivity, including to:

1. declare the impairment and make it transparent. Internal audit will advise on this issue, but implementation is management’s decision and not the responsibility of internal audit;
2. use an alternative internal auditor to review an area where internal audit may have consulted; and
3. use an outside reviewer, somebody who was not involved in the original decision process.

Arguably, too much reliance on the independence issue may be keeping CAE’s away from the top team, forcing them lower down into the management structure and preventing internal auditors from being involved in key issues such as strategy and risk management. Being placed lower in the organisational structure prevents the internal auditors from contributing to decisions, often in areas where they have expertise, which is detrimental to the business overall.

This situation will not be sustainable in the modern rapidly evolving mature organisation. To be accepted as a valued part of the contemporary organisation, the internal auditor needs to be on the executive team, needs to be a part of management decision making and needs to be both strategically focused and also forward thinking.

Alec Richmond, president of the IIA United Kingdom and Ireland (2006, p. 13), believes that independence should not prevent auditors becoming involved in risk management nor keep them away from senior management positions. He cites the similar position of a non-executive director, who on one hand participates in holistic board decision making, while on the other acts as an independent advisor to audit and remuneration committees:
Non-executive directors seem to manage a similar balancing act quite well. They play an active part on the board but then sit on other committees – such as the remuneration committee and the audit committee – as non-executives only.

In summary, studies have found that internal auditors, while seeking independence, often operate in an environment that compromises independence. Adding risk management consulting services to that mix will not compromise an already compromised position. Further, compensating controls, such as a direct reporting line to the audit committee, and the ability to meet privately with the board or audit committee chairman could overcome the above difficulties.

One objective of this research was to explore the role that internal audit independence played in the integration of internal audit and risk management structures.

2.12.3 The Role for Internal Audit in Risk Management

The IIA include risk management in their standards of professional practice for internal auditors. Unlike corporate governance where different countries issue differing guidelines, the IIA is the single major source for standards on internal auditing. The IIA issued the International Professional Practices Framework (IPPF) in January 2009. This framework outlined the definitions, codes, standards and advisories which are adopted internationally by those working in the internal auditing profession.

Under the IAA standards, internal auditors are permitted to become involved in risk management. Practice Advisory 2120-1 outlines the role internal audit can take in risk management. 2120-1 states: “The internal audit activity’s role in the risk management process of an organisation can change over time and may be found at some point along a continuum that ranges from no role to managing and coordinating the risk management process”.
Practice Advisory 2120 requires that the internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes. Internal audit should ensure that significant risks are identified and assessed; appropriate risk responses are selected; relevant risk information is captured and communicated.

A 2006 Australian and New Zealand study by Ernst and Young, which looked at the involvement of internal auditors in risk management, found:

1. forty seven percent of internal audit teams developed and assisted in the oversight of the risk management framework;
2. seven percent of internal audit teams had specific responsibility for managing risk controls;
3. seventeen percent of internal audit teams had some role in providing risk management support;
4. sixty two percent of internal audit teams provided independent assurance over risk management; and
5. 4% of internal audit teams had no role in risk management.

It is clear that internal audit has a lead position in the risk environment and this will help explain why many audit committees appear to be overseeing both internal audit and risk management.

Goodwin-Stewart and Kent (2006) explored the role of the internal audit function in Australian companies. They found that companies with an integrated risk management framework were more likely to adopt an internal audit function and that internal audit is complementary to other risk mechanisms. They also found that the size of the internal audit function is positively correlated to the size of the company.

The IIA and Tillinghast – Towers Perrin in 2001, completed a survey on ERM across international organisations. The survey found that the audit committee was used by 82% of organisations to deal with risk management and compliance issues:
In many organisations, the internal auditing function plays a role in assessing and responding to risks that affect the organisation. Nearly ninety percent of the respondents reported that internal auditing conducts risk-based audits at the business unit level. About one third said that internal auditing participates to some extent on ERM committees or working teams. Approximately one third of the respondents also indicated that internal auditing conducts ERM risk assessments.

Figure 2.7 above, outlines the areas of risk management that are inappropriate for internal auditors. However, an on-line survey conducted by the IIA Research Foundation in 2005, reported that many internal audit teams have responsibilities in these prohibited areas. The situation reported was that internal audit is playing a lead role in the implementation of risk management within these organisations. Whether internal audit can eventually hand these responsibilities over to a replacement function will be seen over time.

In a more recent international study, conducted in November 2008, the IIA also found that 37% of organisations surveyed used internal audit to maintain and manage the organisation’s risk reporting process.

In response to the GFC, a recent IIA roundtable has released a guidance note on how internal audit is changing in response to that crisis. That document stated:

*CAE’s are being asked to take the lead in ensuring that risk management processes are working effectively across the organisation, allowing internal audit to play a key role as strategic partners and champions of risk management.* (IIA, Global Audit Information Network, 2009, p. 9)

Participants at that round table also agreed that “someone with adequate stature must be in charge of organisational risk management” (IIA, Global Audit Information Network, 2009, p. 9). Perhaps the next paradigm shift is already upon us.
The above studies tend to confirm that integration between internal audit and risk management is real and is actually happening despite the independence barrier. It may be that Australian companies are setting up compensating mechanisms that allow internal audit into the risk management function while retaining independence and objectivity. That aspect was explored in this study.

The next section provides solid evidence that integration is occurring on an international scale.

2.13 EVIDENCE OF INTEGRATION

There appears to be a reasonable amount of literature supporting integration between internal audit and risk management, mostly outlining the overseas experience. What is becoming clear is that the move for audit committees to become more involved in risk management is really a broadening of the definition of internal control.

In the old audit paradigm, managers looked at the accounting function and established what could go wrong. Internal control systems were then designed to prevent failures; they were implemented and finally audited. In the new paradigm, which moves away from pure accounting, management identifies enterprise wide risks then designs controls to manage these risks. Audit assists with this process and checks mitigation activity to assure board committees that risks are being appropriately dealt with.

The corporate crashes discussed earlier led to prominent committees such as Turnbull in the United Kingdom and Treadway in the United States bringing some powerful intellect into the governance realm. These committees issued recommendations, which in some cases became law, that required auditors to include risk and compliance in their evaluations of internal control. This now means that the CAE must understand the concepts, systems and processes behind these broader and often non-financial functions.
2.13.1 United States and Canada

In the United States and Canada the internal auditors have embraced the areas of risk management and compliance. The SOX, COSO internal control framework and COSO ERM framework tend to place risk and compliance under the purview of the audit committee and therefore in the hands of the internal audit team.

A recent IIA Research Foundation study as reported by Gramling and Myers (2006) found that in Canada and the United States, 36% of ERM activities were overseen by internal audit, 27% by a CRO and the other third scattered among other different functions such as Finance and Treasury.

Jane Cozzarelli, Vice President of Internal Audit for Battelle Memorial Institute said in Banham (2004, p. 67): “I don’t believe ERM needs to be a separate process with a separate group running it”; and: “once ERM processes are in place, I don’t think there is any problem with audit overseeing them”.

Michael Glotz, Audit Director for Capital One Financial Corporation, in the same article, adds: “in large sophisticated financial service companies, risk management traditionally has its own organisation. It’s really in smaller entities where we’re seeing the chief auditor taking on ERM responsibility”.

Walker, Shenkir and Barton (2002) conducted research to examine how the internal audit function works with management to facilitate the ERM process. This included the identification of tools and techniques and provided examples of reporting structures used by internal audit to report ERM findings. Studying five international corporations, Walker et al (2002) found:

- **Canada Post Corporation** – internal auditors have developed a new integrated risk management process which has transformed the corporation by assisting with the achievement of objectives, managing significant risks and recognising opportunities.
• **FirstEnergy Corporation** – where the risk policy committee and the Manager Enterprise Risk report through to the audit committee. Also the internal audit and ERM departments facilitate risk management on a joint venture basis.


• **Unocal Corporation** – where the risk managers worked in the internal audit department and the General Auditor, Karl Primm changed the internal audit approach from a backward looking compliance approach to a forward looking strategic risk approach.

• **Wal-Mart Stores Incorporated** – Wal-Mart has both a board audit committee and a board ERM committee with risk managers on the audit committee and auditors on the ERM committee. The ERM function sits in internal audit.

Finally, KPMG and the National Association of Corporate Directors (NACD) released the results of their fourth annual survey of United States companies in May 2009. That survey reported (p. 5) that: “Three out of four survey respondents said their board audit committee is reassessing risk management oversight as a result of the financial crisis”. Clearly the integration of internal audit and risk management is taking hold in the United States.

2.13.2 **United Kingdom**

In the United Kingdom there is a similar situation to the United States. Over time the internal audit function has moved from a transaction basis to a risk basis. Starting by using risk management to identify the target areas for audit activity, integration has evolved towards a greater involvement in ERM.
Alec Richmond (2006, p. 13) deputy president of the Risk Management Institute in the United Kingdom discussed the current struggle between compliance and assurance. He saw that struggle as a move to take internal audit away from risk management and focus on only financial compliance routines. He vigorously rejects such a move stating that it will not help prevent corporate failure:

*We know this from the regular surveys of corporate failures that are researched and published by the large accounting firms. These show that focussing all our efforts as internal auditors on financial compliance would miss three quarters of the areas where businesses need assurance that risks are being properly managed.*

The Turnbull review group supports the move of internal auditors into risk management. In the Corporate Governance Group (1999, p.2) Turnbull boardroom briefing paper the working party stated that they saw risk management as a key internal control and that focussing on financial controls only was not sufficient:

“The task ahead is to implement control over the wider aspects of business risk in such a way as to add value rather than merely go through a compliance exercise”. The Turnbull review group reaffirmed the UK commitment to a holistic risk management framework in October 2005.

It seems that, as internal auditors move away from the traditional focus on financial controls, to a more holistic business view, risk management cannot help being swept up in that evolution.

**2.13.3 Australia**

In Australia, Peter Moloney (2005, p. 46) noted:
In the past internal audit and risk management have led separate lives. However, the increased demands that legislation and regulation, such as the ASX Principles 4 and 7, CLERP 9 and APRA Stage 2, have made on companies is making directors and executives more reliant on internal audit for risk management. Internal auditors and risk managers are now regular contributors at many audit committee meetings.

Ernst and Young (2006) have been following Australian and New Zealand trends in internal audit, risk management and compliance in annual benchmarking surveys over recent years. In 2004 the survey looked at how the demands on internal audit had shifted as a result of the HIH and One-Tel collapses. In 2005, the survey continued with the evolution of those demands and in 2006 the survey looked at the trends for risk management practices within organisations. The findings included:

- sixty four percent of respondents indicated that internal audits primary function is to provide risk management assurance, including review and testing of risk management frameworks;
- internal audit has increased its risk management scope in response to an increase in the risk management profile within the organisation; and
- increased expectations of internal audit to provide oversight of risk management has led to an increase in the size of audit teams.

If we turn to information technology, some support is emerging for the integration of risk management and internal audit. Traditionally, the functions of internal audit, risk management and compliance had different sets of system software. Increasingly the major suppliers of these programs are beginning to offer products that cater for a converged assurance environment. The Cura risk management software now offers a compliance module. The 80/20 compliance software offers a risk management module.
This trend seems to indicate that the market is anticipating a convergence of assurance functions.

It is clear that we are seeing integration of the internal audit and risk management in the United States, United Kingdom and Canada. The author’s limited research in Australia also suggests such a change is occurring. Exploring those issues in greater depth was a substantial objective of this research.

Before the gaps in the literature are summarised and developed into research objectives, another potential impediment to an integrated internal audit and risk management paradigm needs to be outlined.

2.14 OUTSOURCING VERSUS CO-SOURCING

This section considers the practice of outsourcing and co-sourcing the internal audit function. These practices have been the subject of heated debate, within the profession for many years. The structure of risk management will be affected by the degree to which a company outsources the audit or indeed the risk management function. In an integrated model, an outsourced internal audit function may have some specific issues.

Many companies do not have an in-house internal audit team. Those companies chose to engage an outside service firm, often a Big Four consulting practice to provide internal audit services. The impact on this study was to see how the outsourcing of internal audit interrelates with the governance models for risk management. On one hand, it will be difficult to integrate an in-house risk management team with an outsourced internal audit function.

On the other hand, the integration of internal audit with risk management may provide the critical employee mass to bring an outsourced internal audit function back in-house.

The decision to outsource internal audit has been well researched. The reasons for outsourcing internal audit are covered by Rittenberg and Covaleski (2001 & 1999) and Selim and Yiannakas (2000).
These motivations are summarized succinctly by Martin and Lavine (2000) who noted cost pressures, the outsourcing of non-core activities, a reliance on global business advisers, personnel flexibility and better quality assurance as factors in favour of outsourcing.

On the other side, having a better understanding of the business, greater loyalty and the provision of in-house management development opportunities are cited as rationale for having an in-house internal audit team. A number of authors (Van Peursem, 2004, Cooper & Craig, 1984, and Myers & Gramling 1997) considered the issue of outsourcing internal audit and the impact on internal audit effectiveness. Those studies argued that outsourced internal auditors will support their “customer” (management) and hesitate to criticise management actions, which creates problems for independence and objectivity.

Aldhizer, Cashell and Martin (2003) saw co-sourcing as the answer. Co-sourcing blends a small core in-house internal audit team with outsourced consultants for: “non-routine services where special capabilities are needed”. Co-sourcing may be as simple as the risk management function, overseen by a CRO, having an outsourced internal audit function handled by a Big Four provider.

Coram, Ferguson and Moroney (2008) found that organisations with an internal audit function are more likely to detect and self report fraud. They also found that organisations with in-house internal audit teams, as opposed to outsourced internal audit, were also more likely to detect fraud.

The Institute of Chartered Accountants in England and Wales (1999) issued guidelines for the implementation of the Turnbull recommendations. Those guidelines recognise that not all companies will have an internal audit function. On page 24, Turnbull is quoted as saying that: “in the absence of an internal audit function, the board will need to assess whether other monitoring processes provide sufficient and objective assurance”.

126
The ASX Principles, while requiring an audit committee, do not require that companies have an internal audit function. Joe Tarantino, when interviewed by Fenton-Jones (2008, p. 56) commented:

_In Australia, the audit committee or board is not mandated to use internal auditors as they are in the US. The IIA – Australia started campaigning vigorously about 12 months ago for internal audit to be mandated in government, corporate and not-for-profit sectors._

In Australia, Goodwin-Stewart and Kent (2006) found that a large portion of Australian companies either do not use internal audit or outsource the function. In that study, completed in 2000, on 450 companies, only 34% of companies used internal audit and 25% of that 34% were outsourced. A similar study by Carey et al (2006) conducted in 1998, found that 33% of companies had an internal audit presence and of that population, 20% outsourced the entire internal audit function.

The Carey study noted above, examined the agency theory determinants of the decision to outsource internal audit. They found that firm size is important when the initial decision to introduce internal audit is made. Smaller firms, when first introducing internal audit tend to use an outsourced supplier to establish the internal audit function. The size of S&P/ASX 200 companies was a factor considered in this study.

A recent survey (2008) of the S&P/ASX 200, was conducted by Regnan Governance, Research and Engagement Pty Ltd, and reported in the Risk Management magazine by A Dix.

Regnan found that only 79% of these leading companies have an internal audit function. The following table highlights these findings:
<table>
<thead>
<tr>
<th>Author</th>
<th>Year</th>
<th>Population</th>
<th>Internal Audit</th>
<th>Outsourced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carey et al (2006)</td>
<td>1998</td>
<td>1030</td>
<td>33%</td>
<td>7%</td>
</tr>
<tr>
<td>Goodwin Stewart &amp; Kent (2006)</td>
<td>2000</td>
<td>450</td>
<td>34%</td>
<td>8%</td>
</tr>
<tr>
<td>Regnan</td>
<td>2008</td>
<td>ASX 200</td>
<td>79%</td>
<td>n.a.</td>
</tr>
</tbody>
</table>

**Figure 2.8 Percentage of companies with internal audit and percentage outsourced.**

This research looked at the extent of outsourcing in the S&P/ASX 200 and how co-sourcing arrangements fit in with the evolving integration of risk management and internal audit.

The next section develops the theoretical approach which can be used to investigate the questions arising from the current debates raised in the preceding sections of this chapter.

### 2.15 RESEARCH OBJECTIVES

Chapter one developed a primary research aim:

*To examine the organisational structure that is used to facilitate risk management in leading Australian companies, including an analysis of the tensions and strengths of integrating risk management with internal audit.*

This section uses the gaps identified in the literature together with the theoretical frameworks discussed above to extend the primary research question into three research objectives.

The primary research question spans structure, governance, board committees, executive management, functional management and the integration of internal audit with risk management.
To adequately address this broad question, three sub-questions are developed that once investigated will move professional understanding of this developing area to a higher level.

### 2.15.1 Research Objective One - Structural Arrangements

To understand the primary question in a little more detail required consideration of the governance structures utilised in leading Australian companies. These governance structures are part of the controls that the owners or principals place over management, the agent. The first and highest level of governance structure is at the board and board committee level. The second level of governance is that of executive management. The final level of governance is the structure at the operational or functional level. The following research objective flows from these governance structures:

*To investigate how risk management is structured at the board committee, executive management and operational levels in leading Australian companies.*

This initial objective gave some direction when looking at the structures for risk management in leading Australian companies. The gaps in the literature pointed to areas where this research can make an original contribution to increasing professional understanding of both risk management and internal audit.

To date there has been little research on the use of combined board audit and risk committees by Australian companies. At a practical level, the smaller size of Australian companies would tend to point towards a combined audit and risk committee. Additional board committees are expensive and Australian companies would be reluctant to incur the additional costs of having separate risk and audit committees. Further, many Australian companies only have three or four non-executive directors. It is hard to split such a small resource over many board committees.
The initial research was therefore aimed at the role of the board audit committee in risk management in Australian companies and the reasons for board audit committees becoming involved in that practice.

That question was tested by conducting a desk-top analysis of Australian companies and by using a survey. A review of annual reports established whether risk management was being governed through a combined board audit and risk committee or separate board committees. The survey provided reasons why such a structure was chosen.

There has been effectively no previous research on the use of separate board risk committees by Australian companies. Not all Australian companies will govern risk management through the audit committee. Contingency theory suggested that different committee structures may have evolved from environmental circumstances. For example, a separate board risk committee may evolve in a financial services environment from a previous credit or loan mandate committee. Different governance structures may result from different environmental factors such as size, industry group or even something as simple as the number of directors available for sub-committees.

The research therefore investigated why some companies set up a separate board risk committee and whether that arrangement was contingent upon environmental factors.

This question was addressed by a desk-top analysis of the annual reports of a selected population of Australian companies and by a survey. The results explored type of committee structure (audit or risk or combined audit and risk) by company size, industry grouping and regulatory framework.

The international literature indicated that integrating risk management into the board audit committee is not without its problems.
Traditionally the audit committee had been primarily responsible for assurance over the annual financial reports. This means that the audit committee member’s require strong financial skills, a point reinforced by the ASX Principles and SOX.

Spira and Page (2002) pointed out that introducing risk management to the audit committee required a new skill set, more time for deliberation and additional training requirements.

Fraser and Henry (2007) argue that, for this reason, internal audit and risk management should be kept apart. Both of these studies were undertaken in the United Kingdom. Research on the skill and timing requirements required when risk management is introduced to board committees has not yet been undertaken in Australia.

The research sought to uncover how leading Australian companies are dealing with the increased skill level, workload and time requirements created by integrating risk management into the board audit committee.

This part of the research methodology was addressed by a survey and follow-up interviews. The survey quantified the issue and asked whether participants would be interested in being interviewed. The interviews dealt with the actions being implemented to address those problems.

Another significant driver for this research is the gap in the literature related to the executive management structure over risk management across the international spectrum. The IIA and Tillinghast – Towers Perrin international 2001 study found that:

- only 30% of organisations have a CRO, with the remainder conducting risk management through the CAE; and
- where CROs exist, the majority came from internal audit departments.
The Deloitte 2004 global risk management survey found that 81% of financial services companies have a CRO; and 50% of all firms have a centralised risk management approach.

To the authors’ knowledge, there are no studies examining the executive structure over risk management in leading Australian companies. No research has been completed to determine the existence of CROs or where they fit into the Australian management structure. This study sought to shed light on the role of CRO and indeed the CFO in the risk management fabric of Australian companies.

Information on CROs could not be gauged from a desk-top review of annual reports. Exploring those questions required a survey of S&P/ASX 200 companies and follow-up interviews.

2.15.2 Research Objective Two - Levels of Integration

The second research objective deals with the relationship between risk management and internal audit in Australian companies. That objective is:

*To establish the levels of integration between internal audit and risk management in leading Australian companies.*

One of the predominant themes of this research was the extent to which the functions of risk management and internal audit are becoming integrated. While there is some literature on this trend at the international level, there is little that has been published on the Australian situation.

Board audit committees appear to be embracing risk management. The literature, in particular McNamee and Selim (1998) and Birkett et al (1997) indicates a trend for risk management to integrate with internal audit at the functional level. The literature provides many examples of risk management combining with internal audit, for example in the United Kingdom (Richmond 2006), the United States (PWC survey 2007) and in Canada (Walker et al 2002).
The research was structured to inform the risk management and internal audit professions on the level of integration between internal audit and risk management in leading Australian companies.

The implications for the research methodology led to a survey approach. Sending a survey to one or more of the CAE, the CRO or the COSEC for each S&P ASX 200 company provided information on these integration issues.

Research on internal audit such as Fraser and Henry (2007) and more specifically the IIA, has identified the maintenance of independence as a defining issue when internal audit and risk management move together. The traditional view is that the internal audit function must remain independent of management in order to report to the board on the performance of management in regard to internal controls.

In contrast, risk managers must work with management, in a facilitation role, to flesh out and mitigate risks to the organisation. When combined, these roles become blurred and internal audit independence will suffer.

The research question that arises for Australian companies is whether maintaining independence is an issue for combined audit and risk management functions and if so, how is this issue being addressed?

This research question required a mix of quantitative survey work and qualitative interviews to determine the extent of the independence problem and the solutions that Australian companies have found to reduce the impact on independence.

The response by regulators to corporate failures has seen a rise in the promotion of risk management. The 2007 version of the ASX Principles recommend a board audit committee as good governance. The same principles, under principle seven, also recommend that companies adopt appropriate risk oversight, risk management policies and risk control systems.
However, much to the chagrin of the internal audit profession, the ASX principles do not recommend that companies establish an internal audit function.

Therefore in Australia, there exists a widely accepted set of governance principles that focus heavily on the requirements for risk management, but fail to support the internal audit function, a function that has for many years been the sole steward of risk management for many companies. Under such a regime, companies will be setting up risk management functions in preference to internal audit functions, relying on the ASX Principles to underpin such decisions.

It is not possible to test this using a desk-top analysis of annual reports. The survey established that some companies exist with risk management but no internal audit functions. Interviews were then required to find out whether such models are becoming more common.

The literature discussed the outsourcing of internal audit and found that various studies (Goodwin-Stewart and Kent 2006, Carey et al 2006) have investigated the reasons for that outsourcing. Part of this research investigated the relationship between the integration of internal audit and risk management when the internal audit function has been outsourced.

A survey question addressed the extent of outsourcing of internal audit in the context of risk management. Interviews were required to establish the impact on governance.
2.15.3 Research Objective Three - Models for Risk Management

Given the research objectives discussed above, some potential models for the governance of risk management in leading Australian companies were developed. Therefore the third research objective is:

*To identify which models are being used to govern risk management in the S&P/ASX 200 Australian companies.*

The models predict the likely make up of the governance of risk management at three levels, the board, executive and the functional or operational level. The following table outlines the three levels of structural governance and the possible drivers for diversity at each level:
<table>
<thead>
<tr>
<th>GOVERNANCE LEVEL</th>
<th>STRUCTURE</th>
<th>DRIVERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Board Committee Level</td>
<td>Combined Risk and Audit Committee</td>
<td>Overseas institutional trends and environmental contingency context:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Size;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Industry;</td>
</tr>
<tr>
<td></td>
<td>Separate Committees</td>
<td>Regulation; and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Specific risk signals</td>
</tr>
<tr>
<td></td>
<td>No Committee</td>
<td></td>
</tr>
<tr>
<td>Executive Management Level</td>
<td>Chief Audit Executive</td>
<td>Overseas trends;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Contingent factors;</td>
</tr>
<tr>
<td></td>
<td>Chief Risk Officer</td>
<td>History;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Entrenched power bases</td>
</tr>
<tr>
<td></td>
<td>Chief Financial Officer</td>
<td></td>
</tr>
<tr>
<td>Functional or Operational Level</td>
<td>Combined Internal Audit and Risk Function</td>
<td>Overseas trends and environmental context;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Contingency outcomes based on factors such as size of firm, maturity</td>
</tr>
<tr>
<td></td>
<td>Separate Risk Function</td>
<td>and entrenched power bases; and</td>
</tr>
<tr>
<td></td>
<td>No internal audit function</td>
<td>Independence barriers.</td>
</tr>
</tbody>
</table>

*Figure 2.9 Models for the governance of risk management*

The literature (KPMG 2005, Subramaniam et al 2009) predicted that a majority of leading Australian companies will combine their audit and risk committees at board level. The remainder will have separate board risk committees due to size, industry grouping, regulation or some type of specific risk factors. There will be some companies with no board risk committee.
At the executive management level there may be a CFO, CRO, CAE or some other executive manager.

The choice may be related to overseas benchmarking (institutional theory), environmental factors (contingency theory) or will have evolved from historical power bases.

At the functional or operational level the model predicts some integration of the internal audit and risk functions, but that a number of different models will exist based on environmental factors. These factors could include the presence of a strong risk executive or the extent to which independence is seen as a barrier.

When developing these models, the attributes of both internal audit and risk management come into play:

1. **Forward versus backward looking**: traditionally, internal audit has been looked upon as a backward looking, compliance, even a “policeman” style of role. Risk management, however, is seen as a strategic, forward looking role that involves modelling future scenarios to ensure that mitigations can be implemented that will help overcome those risks;

2. **Independence**: In some organisations the need for auditor independence keeps the internal audit unit separated from general management and keeps the CAE away from the executive function. Other organisations see the auditors as partners with management.

3. **Maturity**: Immature organisations lack trust and integrity and therefore auditors are required to check on compliance with policy. More mature organisations value integrity and trust and therefore see the auditors as a more strategic partner for management, focussing more on governance than compliance.
The extent to which internal audit and risk management are differentiated by outlook, forward or backward looking, will impact on integration and the model adopted.

The extent to which independence is seen as a barrier to integration will impact on the model utilised. The maturity of the organisation will also impact on integration and possibly on the chosen model.

The next chapter outlines the research methodology that has been adopted to address the primary research aim and the three sub-questions outlined above.
CHAPTER THREE - METHODOLOGY

3.1 INTRODUCTION

The research methodology was designed to address research questions on the board committee and organisational structures that provide oversight for risk management in leading Australian companies. This includes the relationships and links between the governance of internal audit and risk management and contemporary thinking on the interaction between these functions.

The methods chosen to explore the research objectives are outlined in this chapter, together with the rationale for choosing each method. The advantages of, and issues with, each method are also discussed. Situations where similar research has been used by other well recognised researchers are cited to help validate the chosen methodology.

Using a mix of quantitative and qualitative methods the structure of risk management in Australian companies was explored. The methodology ensured the validity and reliability of the study with each section building on the previous and providing validation and triangulation as the study progressed.

The oversight of risk management at board level was addressed by a desk-top analysis of the S&P/ASX 200 companies in Australia. This work was then triangulated with a survey of the same companies. The survey expanded understanding of the management and organisational structures that provide oversight of risk management in the Australian context. Qualitative interviews were added to the framework to explore more deeply the issues and problems that exist with the structure of risk management and the relationships between risk management and internal audit.
3.2 RESEARCH QUESTIONS

A primary research aim and a set of three research objectives were developed from the debates explored in Chapter Two.

The primary research question is:

To examine the organisational structure that is used to facilitate risk management in leading Australian companies, including an analysis of the tensions and strengths of integrating risk management with internal audit.

While much has been written about risk management in general, very little research existed on the board and executive structures that govern risk management. In the author’s experience, combined risk and audit committees were becoming commonplace in Australian companies. Other Australian companies, especially banks and financial services entities were setting up specific board risk committees, in addition to audit committees, to monitor different aspects of risk. The purpose of this research was to examine the board committee, executive and organisational structures within Australian companies with particular reference to the placement of internal audit and risk management. The following sub-questions flowed from the research objective identified in the previous chapter:

Research Objective One - To investigate how risk management is structured at the board committee, executive management and operational levels in leading Australian companies.

Research Objective Two - To establish what levels of integration exist between internal audit and risk management in leading Australian companies:

Research Objective Three – To identify which models are being used to govern risk management in the S&P/ASX 200 Australian companies:
The following section provides an overview of the research methodology that was chosen to explore the research objectives and inform the above questions.

3.3 OVERVIEW OF METHODOLOGY

The research questions and the type of study required to explore those questions determined the research methodology. To answer the above questions a mix of quantitative and qualitative research was required.

The questions about the types of governance committee structures and internal organisational structures that Australian companies are adopting for risk management are objective, descriptive questions of fact. As suggested by Easterby-Smith, Thorpe and Lowe (1991) these questions are best addressed using a quantitative methodology. A desk-top analysis and a survey which focused on the gathering of facts were the chosen instruments.

A desk-top analysis was chosen to report the board risk committee arrangements in the S&P/ASX companies. Some of those companies had risk management oversight from the board audit committee, some had a dedicated board risk committee and a minority had no board risk committee. Since the board risk committee arrangements are reported in the annual reports for each S&P/ASX 200 company, a desk-top analysis was the perfect (and only) choice to capture this publicly available information for 100% of the population. The desk-top analysis involved reading the annual reports for each company and from the corporate governance section, recording the type of board committee structure.

Unfortunately, information on the risk structures under the board level, at the management and functional level is not reported in annual reports. For these “what and why” questions on the board sub-structures, contact with the companies was required. This could be done by survey or by interview.
Trying to gain access to and interview 200 company executives was beyond the resources of this research in terms of cost, time and geographic location. A survey was chosen because that is the most common form of estimating population parameters from a sample population (Weathington, Cunningham & Pittenger, 2012, p 90).

The desk-top analysis and the survey gained structured information, but failed to capture the colour and nuance behind corporate decisions on risk management structure. For this important facet of the research, and to complete the project, semi-structured interviews were conducted with thirty nine corporate executives.

The initial desk-top analysis and survey tended towards a positivist paradigm where quantitative data, statistical methods and objective measures were used to reach findings that are valid and repeatable. Taking a distant, independent and more empirical stance, the research attempted to measure facts on the make-up of audit and risk committees and the organisational and reporting structures for assurance functions within the S&P/ASX 200.

The question of oversight of risk management at board level was addressed by a desk-top analysis of the annual reports of a selected population of Australian companies. The results explored type of committee structure, either separate audit and risk or combined audit and risk by company size and industry grouping. Questions of fact, such as the organisational and management structures that Australian companies use to operate the day to day functions of risk management were addressed using a survey approach.

Armed with these objective measures, the research then moved towards a more subjective methodology. The desk-top and survey analysis led to a number of questions that could only be answered by asking “how” and “why” questions to interview participants. Questions such as:
• You have a combined audit and risk committee at board level because of the synergies between audit and risk. Can you elaborate on these synergies?

• You have a separate board risk committee because you want to focus on some very specific risks. Can you explain these risks and the importance of focussing on them?

• You indicate that your internal audit and risk management functions are integrated. How are you dealing with any independence issues arising from such integration?

Those questions shifted the research away from the positivist paradigm towards a more interpretative paradigm where according to Erickson (1986) interviews become the method of choice. Using interviews, new findings were constructed from the social experiences and perceptions of the executive managers interviewed.

Examples of research successfully using a combination of desk-top or survey and interviews include:

1. Fraser and Henry (2007);
2. Leung, Cooper and Robertson (2004);
3. Covaleski and Dirsmit (1988);
4. Davila and Foster (2007);
5. Wouters and Wilderom (2008); and
6. Graham et al (2005);

The mixing of methodology, quantitative and qualitative, through differing techniques may be advantageous for the research. Easterby-Smith et al (1991) argued that such a mix heightens the research by providing different perspectives on the phenomena under review. Indeed the idea of mixing methods, with each one building on the other and with overlapping questions, helps to triangulate and reinforce the outcomes of the different research methods outlined above. This combined approach is also supported by Burgess (1991) and Denzin (1989) who argue that this is the best way to conduct a research project that involves human interactions.
The integration of desk-top or survey and interviews, a form of mixed method, has grown in popularity over recent years (Hall and Howard, 2008, Denscombe, 2008). Generally, mixed method involves combining both quantitative methods with qualitative methods into a single study (Cresswell and Plano-Clark, 2007, Hall and Howard, 2008). The overall aim is for the different methods to reinforce or “triangulate” with each other, identifying overlapping outcomes, possible contradictions and extending the findings. The blending of methods will provide a richer outcome by balancing the strengths of one method against the weaknesses of another (Jick, 1979).

Not all researchers are in favor of mixed methods. There exists a school of thought that qualitative and quantitative methods should not be combined. This “incompatibility” view (Brannen, 2005, Scott and Briggs, 2009) argues that the different epistemological assumptions behind each method, prevents integration. To attempt a combination of positivist external reality with an interpretivist reality constructed by the participants will lead to tension and an inability to interpret results (Grafton, Lillis and Mahama, 2011). In contrast, a pragmatic school of thought argues that research questions drive the methodology and those questions can require both a quantitative and qualitative approach (Brannen, 2005, Bryman, 2007). The rationale, rather than the epistemology should drive the research (Scott and Briggs, 2009, p 231).

Jick (1979), Modell (2005) and Johnson and Turner (2003) outline the following benefits from mixed method studies:

1. Using more than one method can extend the findings;
2. Empirical contradictions can be identified;
3. Different methods can reinforce one another, thereby increasing confidence and validity; and
4. The data can be richer and thicker.
Piantanida and Garman (2009, p 83) add that another valid justification for mixing methods is the value added from understanding complex phenomena from multiple world views.

In this study, the desk-top was completed using the full population of the S&P/ASX 200. The survey produced a sample of these 200 companies and triangulation with the desk-top helped increase validity and reliability and also provided proof of a lack of non-response bias. The interviews, when integrated with the survey outcomes provided much richer explanations of the findings and the reasons behind those findings.

Before moving into the detailed methodology, the choice of the appropriate population requires consideration.

3.4 THE S&P/ASX 200 COMPANIES

One of the major difficulties with research projects on Australian companies, as outlined by Silverman (1993) is the sheer size of the undertaking. Aiming the research at the entire population of Australian listed companies, nearly 2000 companies would be a very difficult and expensive task.

The S&P/ASX 200 companies is a more manageable and appropriate population. As outlined in the S&P Australian Indices: Index Methodology (2006), the S&P/ASX 200 represents the more significant companies in terms of size and impact on the Australian business fabric. These leading companies would be using structures that are designed to give them the best results within the constraints of their operating environment.

The S&P/ASX 200 was chosen as a manageable set of Australian companies, a set that includes many of the best performing companies. Established in April 2000, the S&P/ASX 200 was designed to provide institutional investors, mutual fund managers and professional advisers a liquid, tradeable and easily replicated index.
According to S&P “the S&P/ASX 200 is closely aligned with the S&P global suite of indices, and is recognised internationally as Australia’s principal investable equity index”. The index covers eighty percent of the Australian equity market by capitalisation, with a constituency that is highly liquid and tradeable. The high degree of institutional shareholder involvement in the S&P/ASX 200 places additional pressure on these companies to adopt high standards of governance.

It makes sense, when looking for trends in governance, to investigate these more attractive Australian companies. These companies tend to be the more successful, better recognised companies that other companies seek to follow and look to for benchmarking and guidance.

The question of whether the findings from this population can be generalised to the wider set of all Australian listed companies is important. The study has not asserted that this population is representative of all Australian companies but suggested that being included in the S&P/ASX 200 is something that most Australian companies aspire towards. The findings with respect to structure and governance may well be the practices that other companies are moving towards.

This is in keeping with the mimetic isomorphism outlined by DiMaggio and Powell (1983). Risk management is a new technology being adopted in an increasingly uncertain environment. This gives rise to the conditions noted by DiMaggio and Powell where organisations seek to implement similar practices to those adopted by acknowledged industry leaders.

The next sections provide a detailed explanation of each of the three stages developed to inform the research questions:

**Stage 1** - a desk-top analysis of the S&P/ASX 200 companies as at the 30 June 2007: completed between July 2007 and December 2007;
Stage 2 - a survey of the same S&P/ASX 200 companies: completed between April 2008 and September 2008; and

Stage 3 - interviews with senior executives from the above S&P/ASX 200 companies over the period August 2008 to November 2008.

The population for the desk-top analysis in Stage 1 was the entire S&P/ASX 200 set of Australian companies. There was no sample, as information on the full population was available from public sources. In the Stage 2 survey, the population consisted of the S&P/ASX 200, but the survey responses constituted a sample of that population. In Stage 3, the qualitative interviews, the population consisted of the S&P/ASX 200 and the interview respondents became the sample. The interview sample was not statistically representative of the population, but that is a common issue in qualitative studies (Berg, 1989). The interview responses however, provided detailed rich information which helped inform the more statistically reliable and valid survey and desk-top results.

3.5 STAGE 1 – DESK-TOP ANALYSIS

The first stage of the research was to ascertain the board committee structure for the S&P/ASX 200 companies with respect to risk management. This was a question of fact, at the positivist end of the paradigm spectrum, and suited a quantitative desk-top analysis of annual reports and published governance statements.

The companies comprising the S&P/ASX 200 move over time. While the S&P and the ASX try to minimise that movement, companies are continually being added and removed as they meet, or fail to meet, the criteria. Therefore, to lock down a point in time, the data-set comprised the S&P/ASX 200 companies as at 30 June 2007 (see Appendix One). The annual reports for those companies with a 31 December 2006 financial year end (FYE) whose reports came out in March 2007, were analysed between July 2007 and September 2007.
For those companies with a 30 June 2007 FYE, the latest data was added between September 2007 and November 2007 when the annual reports were published around September 2007.

Using the latest annual report for each company which included either a December 06 or June 07 FYE, the following information was recorded as the data-set:

<table>
<thead>
<tr>
<th>ABBREVIATION</th>
<th>VARIABLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>COY</td>
<td>Company Name</td>
</tr>
<tr>
<td>ASX</td>
<td>ASX Security Code</td>
</tr>
<tr>
<td>GICS</td>
<td>Global Industry Classification</td>
</tr>
<tr>
<td>REV</td>
<td>Revenue in A$ million</td>
</tr>
</tbody>
</table>
| ADR          | 2 = Board audit and risk committee  
|              | 1 = Separate board risk committee  
|              | 0 = No board risk committee |

**Figure 3.1 Classification of variables – desk-top analysis**

From the annual reports and in particular the corporate governance statements in the annual reports, the board committee structure with respect to risk management and audit (ADR) was obtained. Three different types of structure existed:

1. a combined board audit and risk committee;
2. two separate board committees, one for audit and one for risk management; and
3. no board risk committee.

The Global Industry Classification (GICS) and the revenue (REV) for each company were also obtained from the annual reports. These variables helped explain the type of board committee structure adopted by different companies.
For example, it was found that separate board risk committees are more common in the highly regulated financial services industry (GICS, 40). Goodwin-Stewart and Kent (2006) and Carcello et al (2005) both found a relationship between “risky” financial institutions and the existence of an internal audit function.

Revenue (REV), in million dollars, was chosen as an indicator of company size. As found by Subramaniam et al (2007) larger companies, as indicated by revenues, may have both the resources and sufficient directors to allow separate audit and risk committees at board level. Smaller companies might tend to integrate the CAE, CRO and even the CFO positions as a cost saving measure. Revenue has also been used by Kleffner et al (2003) and Beasley et al (2005) as an indicator of the relative size of the company when examining agency related factors.

Subramaniam et al (2009) used a similar desk-top methodology to study the relationship between board factors and the existence of board risk committees in Australian companies. In that study, the 2005 annual reports for the S&P / ASX 300 companies were reviewed for the existence of board risk committees. Independent variables used in that study included industry classification and the size of the company as measured by total assets.

In this study, revenue, rather than total assets, as used by Subramaniam et al 2009, is used as a surrogate for size, for two reasons:

1. Finance theory, Brealey and Myers (2003), suggests that a firm’s value is underpinned by the quantum of free cash flows, largely revenues; and

2. While total assets can be large, these assets are often offset by large quantities of debt. The global financial crisis has shown us that excessive debt is neither a sustainable position nor an indicator of company size.
Rather than total assets, revenue was considered the more appropriate indicator of company size.

Covaleski and Dirsmith (1988) used a desk-top analysis of university budget papers and submissions, followed by interviews to examine how stakeholders impact on the University budgetary process.

Goodwin-Stewart and Kent (2006) used a combination of desk-top and survey information to identify factors that lead to the appointment of internal auditors. A desk-top analysis identified publicly available agency information such as size, profitability and risk. The survey built on this information to flesh out aspects of the internal audit and risk management functions.

Liebenberg and Hoyt (2003) also used a desk-top analysis of publicly available information in their study of the appointment of CROs. That study used media announcements (Lexis-Nexis, Dow Jones and PR Newswire) to identify companies that had signalled the appointment of a CRO. A desk-top analysis of annual reports, aimed at identifying agency related factors, was then completed for the identified sample.

On their web-sites, many of the S&P/ASX 200 companies provided details on the charter for their board audit and risk committees. These are provided to satisfy the corporate governance information required under the ASX Principles. Where this information was provided, copies were recorded for later research analysis.

As the research work proceeded, notes were also kept on whether internal audit appeared to be outsourced, and whether CAE or CRO executive positions were evident. A copy of the data-set achieved is attached as Appendix Two.

It is argued that this style of research is both reliable and valid. If another researcher repeated this desk-top analysis at the same time, the results would be identical. The passage of time may shift the outcomes as companies change their risk management structure, however such change involves board and executive consideration and is therefore slow to evolve.
The issue of reliability is enhanced by the data-set being extracted from actual audited annual reports rather than the thoughts or opinions of survey respondents. Sample size and representativeness to a population are not an issue since the entire population of S&P/ASX 200 is being used for the desk-top data-set. There appears to be no ethical issues with this section of the analysis as all information is publicly available.

The desk-top analysis allowed access to publicly available information that answered questions of fact:

- What is your industry segment?
- What is your revenue?
- Do you have a combined board audit and risk committee?
- Do you have a separate board risk committee?
- Do you have any board risk committee?

The data-set resulting from the desk-top analysis was termed the “desk-top data-set” and was entered into Excel as a relational database. That data-set is discussed in the data analysis section later in this chapter. A copy is included as Appendix Two.

Finally, the information gained in the desk-top analysis underpinned the next section which considers why companies are using different risk management structures at different levels of governance. The survey work in the next step was triangulated with the above desk-top data-set using overlapping questions on board committee structure and revenue. The work from stage one was combined with stage two to give an overall picture of risk management structures in leading Australian companies.
3.6 STAGE 2 - SURVEY

The next stage of the research sought answers to questions, the answers to which are not publicly available. In essence, communication with the companies was required. Also, the questions started to merge both fact and opinion:

- Can you confirm your revenue?
- How mature is your ERM adoption?
- Why do you have a combined board audit and risk committee?
- Why do you have a separate board risk committee?
- Who is the executive overseeing risk management?
- How is your internal audit function set-up?

To extract information on these “what is the situation” and “why do you do it” questions, a methodology was required that allowed communication with a large population in a reasonable timeframe and at moderate expense.

Dillman (2007, p. 5) showed that the survey technique is capable of handling a larger population at reasonable expense. However, care needs to be taken with a number of issues associated with surveys. Cooper and Schindler (1998) outlined the problems with survey analysis, including issues relating to the population and sample selection and issues relating to survey design and data collection.

3.6.1 Population and Sample Selection

Care needed to be taken so that the response rates could be statistically related back to the full population. For example, Beasley et al (2005) used an electronic survey approach to examine the factors associated with the adoption of ERM in United States firms. Beasley used the IIA, Global Audit Information Network (GAIN) to survey seventeen hundred CAEs which resulted in a 10.3% response rate.
In Canada, Kleffner et al (2003) used a mail survey of members of the Canadian Insurance and Risk Management Society (CRIMS) to examine the adoption of ERM in Canadian listed companies. They obtained a 35% response rate. In Australia, Carey et al (2006) surveyed 1030 ASX companies to investigate the determinants of internal audit outsourcing in Australian firms. The study achieved a 30% response rate.

In research conducted by Leung et al (2004) into the governance oversight of internal audit in Australia, the population was assumed to be all entities with an internal audit presence. The sample consisted of the 397 CAEs registered as members of the IIA in Australia. The response rate for the survey was 85 usable responses or 21%. Leung et al (2004, p. 9) note that “the response rate is reasonable based on typical response rates from research of a similar nature”.

In this research the S&P/ASX 200 is the entire population and all are being surveyed, hence there is no issue with choosing a sample size. However, as noted by Tabachnick and Fidell (2001), response rates will be important to allow statistical generalisation from the responses back to the S&P/ASX 200 population. High response rates were achieved for the survey by following the Dillman (2007) methodology for mail surveys. Those steps are outlined in the following survey section.

3.6.2 Data Collection

The literature reveals that a number of issues can arise from the survey design and data collection.

The survey needs to be kept simple to avoid the “mess, clutter and confusion” which Babbie (1990) and Wadsworth (1997) suggest leads to lower response rates. Leung et al (2004) used an online survey containing 55 questions, which is arguably too many for busy recipients, to gain a 21% response rate.
Kleffner et al (2003) had about half this number of questions and ended up with a much higher response rate at 35% when compared with the Leung et al study.

On a similar theme, the Kleffner study questionnaire opened with simple, basic questions on demographics to gain the respondents confidence. The Leung et al study commenced with complex questions on the content of audit charters.

3.6.3 Design of the Survey Questions

Pilot interviews help the researcher understand the limitations of different methods and also assist with question design and the approach to participants (Dillman, 2007, p 146). This study was preceded by a set of pilot interviews which helped establish the research questions and the sub-categories within those questions.

Sapsford (2007), Dillman (2007), Greer, Chuchinprakarn and Seshadri (2000) suggest a number of principles aimed at making surveys more user-friendly, and improving response rates, while using modern communication channels. The design of the survey questions was guided by these suggestions. A brief outline of these principles is attached as Appendix Nineteen.

The survey for this research was designed to provide answers to the questions that flowed from the three research objectives outlined in Chapter Two. A matrix which cross-linked each research question to a survey objective was developed by the researcher and is attached as Appendix Five. Appendix Three provides a copy of the actual survey instrument used.

Using Sapsford (2007), Dillman (2007) and Greer et al (2000) suggestions resulted in a set of interesting questions, each of which was linked to the research objectives and research questions. The survey is attached as Appendix Three and Appendix Twenty One provides a rationale for each question.
3.6.4 Design of the Survey Format

As with the design of the survey questions, a number of writers provide valuable insights into the design and format of the actual survey (Sapsford, 2007 and Dillman, 2007). These suggestions cover the length of the survey, style, front cover design, instructions, layout, navigation and the design of “skip” questions. Appendix Nineteen provides a summary of Dillman’s survey design suggestions.

The author followed these suggestions and chose a booklet style of survey document with an easy lead-in question, careful ordering of the “skip” questions with clear instructions using bolder fonts. Navigation pathways were included throughout the survey.

The author had a choice of using telephone, on-line (Leung et al 2004) or mail survey methodologies. A mail survey was chosen because neither the e-mail addresses nor telephone numbers for S&P/ASX 200 Company Secretaries are available as public information. The name and mailing address of each Company Secretary is listed in the information provided by the ASX listing requirements. Also Leung et al allude to the impersonal nature of on-line surveys. In that research, they sent personal e-mails to respondents and promoted IIA endorsement to overcome the problem.

3.6.5 Validation of the Survey

Once initially designed, the survey was then exposed to a quality assurance (QA) or validation exercise. This type of exercise is advocated by the IIA and would be used by the author before engaging in a survey for internal audit purposes. The validation involved:
1 review by the risk and audit team from a leading Tasmanian utility;

2 review by two Big Four partners, one in Hobart, and one in Melbourne;

3 review by Ian Farley and Associates, a Tasmanian based commercial survey business;

4 review by EMRS Marketing, a Hobart based marketing company, see Appendix Sixteen; and

5 a pilot survey was then conducted using five large Tasmanian businesses.

The Hydro Tasmania Assurance Group helped with spelling, grammar and making sure that the wording was simple. This exercise also helped ensure that the “skip” questions worked and that all possible combinations of possible answers were covered. Two Big Four risk experts assisted with the alternative answers for the questions with Likert scales, and the ordering of the questions, which needed to flow as the survey progressed.

The review by Farley and Associates resulted in changes to the order of the questions and changes to the wording for the skip questions. The review also confirmed that the survey, as presented, would help inform the research questions. The review by EMRS confirmed that the survey aligned with the research objectives, was logical and that the language was clear and appropriate. A copy of the EMRS report is attached as Appendix Sixteen.

Each of the above steps led to fine tuning, most of which was aimed at reducing ambiguity and increasing both simplicity and clarity.

A pilot survey was used to test the instrument on a selection of five Tasmanian Company Secretaries and Senior Risk Managers. This led to some changes in emphasis and wording. The pilot showed that some risk concepts, such as ERM are not well understood, which led to more emphasis on definition.
The pilot also showed that the definitions of “outsourced” versus “co-sourced” internal audit required greater clarity. The pilot confirmed that the survey should take no more than twenty minutes to complete. The pilot also confirmed that nothing ambiguous was included in the survey. Pilot surveys are advocated by Dillman (2007, p. 146) to “reveal ways of improving the questionnaire”. Carey et al (2006) used a similar pre-test methodology. They pre-tested their survey on five academics from two universities and directors of two large private companies. The pre-tests resulted in modifications.

It is important to note that the sample size (S&P/ASX 200) had reduced over the twelve months since the 30 June 2007 date established for the desk-top analysis. Twenty seven companies had either, been merged, taken over or de-registered during the period 30 June 2007 to 30 June 2008. Since the research required the same companies be included in the desk-top and survey analysis for triangulation, the population for the survey was reduced to 173 S&P / ASX companies.

Approval for the survey work and for the interviews outlined in the next stages was obtained from the Charles Sturt University (CSU) Ethics Committee in November 2007 (see Appendix Fifteen). Ethics guidelines were provided to all recipients of the survey as part of the CSU required information statement (see Appendix Eight). Page 9 of the survey (see Appendix Three) requested involvement in a short interview. Only those executive who agreed to be interviewed were contacted.

Dillman (2007) recommends the following contact steps to help increase response rates for mail surveys:
1. a brief pre-notice letter, sent out several days before the survey (see Appendix Seven);

2. the questionnaire mailing, which includes a covering letter explaining why the research is important;

3. a thank you post card is sent a week after the questionnaire, expressing appreciation and encouraging completion;

4. a replacement survey is sent four to six weeks after the previous mailing (see Appendix Nine). This indicates that the completed questionnaire has not been received and prompts for a response; and

5. a final contact, perhaps using a different mode of contact, such as e-mail or telephone, is made two to four weeks after the last contact.

Following Dillman’s (2007) principles, on 6 May 2008, a pre-notification letter was sent to the Company Secretaries for all S&P/ASX 200 companies that were listed as at 30 June 2007 and were still listed at that point in time.

The letter informed the participants of the coming survey, provided background to the research and included a copy of the first article published about this research in the Risk Management magazine, see Appendix Seven.

A copy of the survey, which included an introduction letter, was mailed to the Company Secretaries of each organisation on 21 May 2008. The letter introduced the author, outlined the purpose of the research and indicated support from Charles Sturt University (Greer & Lohtia 1994). The letter of introduction (see Appendix Eight) also outlined the confidentiality arrangements. Importantly, assurance was given that no respondent nor any company names or identifying features would be revealed in the study. All outputs would refer only to aggregated or industry sector information. The researcher knows which company has provided what information, but that information has been and will continue to be kept confidential and secure.
As an incentive (Hansen, 1980) and as a thank you, (Newby, Watson & Woodliff, 2003) respondents were offered access to the results of the study upon completion. Respondents were also asked whether they would be willing to participate in a telephone interview at the next stage of the study.

A follow up letter was despatched on 30 June 2008 followed by a second on 31 July 2008. For companies that had not responded by the end of July 2008 after four unsuccessful contacts, surveys were then sent to the alternative COSEC, CRO, CFO or CAE, depending on the information known about those companies. This turned out to be particularly effective. Post June 2008, the COSECs were becoming heavily involved in their annual reporting requirements. Completing a survey was the last thing on their minds.

The alternate risk executives CFO’s, CRO’s and CAE’s on the other hand, had more time to engage. Some Company Secretaries completed their surveys after finishing year end and those surveys were received in October and November 2008. Multiple responses were not received from any company.

Overall, 102 valid survey responses were received from a population of 173 companies. This gives a response rate of 59% for the survey section of the research. This compares favourably with response rates for similar work, targeting such executives (Christopher et al 2007 (17%), Bariff, 2003 (22%) and Leung, Cooper & Robertson, 2004 (21%)).

Non-response bias is a consistent tendency for the survey results to be higher or lower than the results for the full population (Andrews, 1984, p. 410). Non-response bias would occur, if, for example, the survey respondents were all from the smaller companies in the S&P/ASX 200. In such an example, the larger companies would be poorly represented, skewing the results of the findings towards the smaller company characteristics.
Non-response bias was partially controlled by the high response rate achieved from the survey. Intuitively, the higher the response rate the less likely that non-response bias will be a limiting factor. Given a response rate of 59%, nearly three times the rate achieved in similar studies, the problem of non-response bias became much less of a problem.

To check that non-response bias was not impacting the results, two factors were compared between the survey responses and the full population. Firstly, the percentage of companies in each GICS was compared between the full population and the survey population. This assessment made sure that no one particular GICS was over or under represented in the survey. The following table outlines the results of the GICS non-response bias testing.

<table>
<thead>
<tr>
<th>GICS</th>
<th>Desk-top S&amp;P/ASX 200</th>
<th>Survey S&amp;P/ASX 200</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 - Energy</td>
<td>7%</td>
<td>6%</td>
</tr>
<tr>
<td>15 - Materials</td>
<td>19%</td>
<td>13%</td>
</tr>
<tr>
<td>20 - Industrial</td>
<td>15%</td>
<td>25%</td>
</tr>
<tr>
<td>25 – Consumer Discretionary</td>
<td>13%</td>
<td>14%</td>
</tr>
<tr>
<td>30 – Consumer Staples</td>
<td>4%</td>
<td>5%</td>
</tr>
<tr>
<td>35 - Health</td>
<td>4%</td>
<td>4%</td>
</tr>
<tr>
<td>40 - Financial</td>
<td>26%</td>
<td>22%</td>
</tr>
<tr>
<td>40 - IT</td>
<td>1%</td>
<td>1%</td>
</tr>
<tr>
<td>50 - Telecoms</td>
<td>2%</td>
<td>2%</td>
</tr>
<tr>
<td>55 - Utilities</td>
<td>6%</td>
<td>9%</td>
</tr>
<tr>
<td>TOTAL</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

*Figure 3.2 Controlling non-response bias*
While GICS 20 (Industrials) is over represented in the survey responses, all the remaining GICS have survey percentages close to the full population. The similarity between the percentage of companies in each category helps confirm that non-response bias is low.

In addition, as an added check, the survey response companies were compared to the full population of the S&P/ASX 200 in regard to the following categories:

1. The percentage of companies with a combined board audit and risk committee;
2. The percentage of companies with a separate board risk committee; and
3. The percentage of companies with no board risk committee

Those results are outlined in Section 4.2, as part of the triangulation between the desk-top and survey analysis. The alignment between the percentages of companies in each category is also confirmed by a Chi Square test.

A copy of the data-set resulting from the survey, which includes the Likert scales, is attached as Appendix Four. This data-set was then synthesised into a set of dependent and independent variables by removing the Likert scale questions. The scale questions, which provide a more qualitative response, were dealt with separately. The survey data-set explored the following variables:
<table>
<thead>
<tr>
<th>ABBREVIATION</th>
<th>VARIABLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASX</td>
<td>ASX Security Code</td>
</tr>
<tr>
<td>ADR</td>
<td>Audit and risk arrangement at board level</td>
</tr>
<tr>
<td>REV</td>
<td>Revenue in A$ million</td>
</tr>
<tr>
<td>YRS</td>
<td>Years since incorporation (gives an idea of the age of the company)</td>
</tr>
<tr>
<td>GICS</td>
<td>Global Industry Classification</td>
</tr>
<tr>
<td>ERM</td>
<td>Maturity of ERM system</td>
</tr>
<tr>
<td>EXO</td>
<td>Executive responsible for risk management</td>
</tr>
<tr>
<td>FUN</td>
<td>Functional arrangement audit and risk</td>
</tr>
<tr>
<td>IAU</td>
<td>Internal audit arrangement</td>
</tr>
</tbody>
</table>

**Figure 3.3 Classification of variables - survey analysis**

The data-set resulting from the survey was entered into Excel as a relational database. That data-set is discussed in the data analysis section later in this chapter (see Appendix Four).

While the above information provided an objective snapshot of what types of organisational structures existed, it only partly answered why such structures were chosen and why other options were not considered appropriate by companies. At that point the study moved towards a more subjective analysis.

The questions arising from the desk-top analysis and survey underpinned the next stage where qualitative interviews were undertaken to document a management perspective on these key issues.
3.7 STAGE 3 - INTERVIEWS

3.7.1 The Need for Interviews

The desk-top analysis in stage one provided quantitative data such as the number of S&P/ASX 200 Australian companies that have combined board audit and risk committees. The surveys in stage two confirmed that number and focused on the reasons for that particular arrangement. The next step was to introduce a more qualitative analysis to help understand the motivations behind particular arrangements. As an example, the results of the desk-top analysis indicated that the majority of companies have a combined board audit and risk committee. The survey responses received indicated that the synergies between audit and risk management are the main driver for having a combined audit and risk committee. Qualitative interviews were then required to understand exactly what is meant by these synergies.

The quantitative findings from the desk-top and survey work have their origins in a realist ontology, which subscribes to the view that “the real world is out there and exists independently from us” (King and Horrocks, 2010, p. 9).

The desk-top and survey consisted of measurement and numbers that report on the organizational structures that exist at a point in time. When turning to the motivations and behaviours that are behind and drive these structures, the experiences and understandings of executive managers were required.

This moved the study from a realist perspective to more relativist ontology, sourced from interpretivism. Interpretivism is concerned with how people experience and understand the world around them (Holliday, 2002). To move from realist to relativist requires interaction with people “generally in a face to face situation” (Lapan, 2012, p. 85).
The qualitative research interview is the most commonly used method of data collection in social research, leading Gubrium and Holstein (2002) to claim we are now in an “interview society”.

### 3.7.2 Interview Techniques

Fontana and Frey (1994) outline the types of interview technique that can be used for this type of research. These techniques can be summarised as a continuum ranging from the inflexible “structured” approach to a much more interactive “unstructured” approach.

The structured approach is more suited to using interviews to quantify survey data. This approach uses set questions, a predetermined coding system for answers and allows little flexibility. The interviewer does not deviate from the questions, does not assist the interviewee to answer questions nor attempt to interpret meanings. The structured approach is aimed at minimising interpretational errors (Converse & Schuman, 1974). However, the structured approach may overlook or inadequately assess any emotional dimension, (Fontana & Frey, 1994).

At the other end of the spectrum comes the unstructured approach. Unstructured interviews involve the interviewer and interviewee working together to interpret reality. This involves deviation from the original questions, suggestions from the interviewer, interpretation and clarification of meanings and improvisation.

The unstructured approach is more open to criticism for validity concerns, where the interviewer may lead the interviewee. On the other hand, the unstructured approach “can provide rich insight into human behaviour” (Guba & Lincoln, 1994).

### 3.7.3 Chosen Technique

In this research a semi-structured approach has been adopted. Since one aim of the interviews was to validate the desk-top and survey findings, the interviewer used a set of predetermined questions based on the survey outcomes.
However, since the author also wanted insights and perceptions into the research questions, some unstructured elements were added. For example, deviation from the questions was allowed, the meanings of the questions were often debated and interviewees were encouraged to provide insights and perceptions.

Fraser and Henry (2007) undertook a similar methodology to study how companies identify risks and to report on how audit committees contribute to risk management. That study commenced with a review of the literature on audit committees and risk management and then used interviews with senior executives from United Kingdom companies together with external auditors to discuss issues identified in the literature. Fraser and Henry (2007, p. 399) chose this method because “unstructured interviews were regarded as the best approach to tease out information on perceptions and experiences” and “enable the exploration of the richness of the issues”.

In a similar manner Leung et al (2004), while using a structured approach, designed their questions so that “maximum opportunities were given to interviewees to express their views and insights from their own experience” with simple leading questions like:

- “What policies exist (or are proposed) within the organisation to support effective corporate governance?”; and
- “What processes are in place to administer the day-to-day running of the organisation and support the delivery of effective corporate governance?”

### 3.7.4 Problems with Interview Techniques

A set of pilot interviews were conducted with leading Tasmanian risk practitioners in April 2006. These interviews were aimed at risk management structural issues and were designed to help establish the key objectives for this research. The outcome of the pilot indicated:
• it is very easy for the interviewer to lead the interviewee – control comes from having a pre-arranged list of questions and prompts;

• only four or five questions can be addressed in a 20 minute interview; and

• The other difficulty encountered was the nexus between the interview questions and the research questions. It was easy to be led, in discussions with the interviewee, away from the direction required by the research question. This point is confirmed by Glesne (1999, p. 69) who points out that time and energy need to be devoted to developing the interview questions “that are related, but not equal, to your research questions”.

Berg (1989) supports the above findings by outlining the following key issues with the interview method;

• the wording and delivery of the questions create situations where researcher bias is an issue;

• the issue of validity and reliability, that is, can any generalisation be made from a small sample of interviews;

• logistical and ethical issues, which include entry, exit, follow-up, recording and transcription, to name but a few; and

• choosing the correct data analysis technique from a myriad of options, most of which have their origins in human science.

Denzin (1989) indicated that the more structured the interview question, the more likely that interviewer bias (putting words in their mouth) may occur. A good example of this is one of the questions asked in the interviews conducted by Fraser and Henry (2007) in their research into the relationship between audit and risk management.
The question; “What should be the role of Audit Committees in risk management given the limited time and expertise available to carry out more than a high level overview of the risk management process?” imposes a strong message to the interviewee that there are problems with Audit Committees getting involved in risk management.

The interviews used in this research were designed around the simpler style adopted by Leung et al (2004). Starting with broader more general questions then focusing in depth based on the interviewee responses and using prompts for clarification. If an interview respondent wanted to move off on a tangent, to provide a personal view on an issue, that divergence was supported.

Often these transgressions highlighted a particular issue that was important to the study and was of significance to the interviewee. This approach is suggested by Hirst and Koonce (1996, p. 460) and was used by Cohen et al (2002) in their interviews on governance and the audit process. Fraser and Henry (2007) also used this approach in their interviews on the identification of risks and processes to embed risk management.

One of the primary concerns with the interviewing method is sampling, that is, validity and reliability may be compromised in small scale interviews that cannot be generalised to the wider population (Eriksson and Kovalainen, 2008). In this work, no attempt is made to generalise the results of the interviews to the full S&P/ASX 200 population. Rather, the interviews provide a rich source of information that supports and elaborates on findings from the desktop and survey results.

Once again, the work on risk management by Fraser and Henry (2007) may provide insight into the above problem. Using interviews with only seventeen respondents, without any accompanying survey, Fraser and Henry (2007, p. 407) conclude that:
“We recommend the creation of dedicated risk management functions, while internal audit concentrate on monitoring the adequacy and effectiveness of systems operation”. There appears to be a huge leap from seventeen arguably biased interviews to the whole population of United Kingdom public and private companies.

Again, in contrast, Leung et al (2004, p 9) transparently set out in their methodology to “cover a range of organisations, big and small, national and international, drawn from private enterprise and the government sector across Australia”. Although Leung et al (2004) interviewed only twenty five people, the interviews were followed by an extensive survey, which provided the base facts. The interviews were designed to “gain a further understanding of the research issues from a business perspective” (p. 9) and were not taken to be representative of the wider population.

The interview design for this research was aimed at fleshing out issues that arose or required clarification from the survey providing the insights of the respondents in a rich and more descriptive manner. Responses from participants were arranged into common groupings and quotes were used to both highlight and support findings.

Buchanan, Boddy and McCalman (1988) outlines practical strategies to overcome some of the logistical issues that arise during interviews such as recording interviews, transcripts, correspondence, confidentiality and relationships with the interviewee.

However, they advocate an opportunistic approach where a fastidious attachment to rigour must be softened by the practicalities of each situation.

Leung et al (2004) provide some strong examples of overcoming logistical and ethical problems. In their interviews with CAE’s they ensured that access to the data and the identities of the interviewees remained with the researchers thereby maintaining anonymity and protecting the integrity of the research.
Every interview was preceded by a preliminary phone call to explain context and the purpose of the meeting. This was followed by an email that again outlined the context and the framework for the meeting. At the start of the meetings the interviewee was again made aware of the purpose of the research, the value of the benchmarking data and a pledge of confidentiality.

The interviews conducted in this work were guided by the methodology used by Leung et al (2004).

3.7.5 Interview Questions

A review of the data-sets developed in stage one, the desk-top analysis, and stage two, the survey data-set, clearly showed what questions were required for the interviews. These questions were all designed to expand on, and triangulate the information received in the earlier stages. The questions were categorised into eight areas:

**Question One**

*You have a combined board audit and risk committee due to the synergies between audit and risk. Can you please elaborate on these synergies?*

This question came from responses to question four in the survey where the majority of respondents identified “synergies between audit and risk” as the reason for bringing risk management under the wing of the audit committee.

Many of these respondents tried to explain the synergies in the brief space given for comments on the questionnaire. For example: “There is a synergy, we adopt the three lines of defence model”.

**Question Two**

*You have a separate board risk committee to focus on issues specific to your business. Can you please elaborate on the importance of these issues?*
Question six from the survey indicated that a number of companies had chosen a separate board risk committee to focus on specific risks. The interview question was designed to reveal the nature of those risks and why they are more important than other risks. The question also revealed that signalling was an important factor in the decision on the structure of the board risk committee.

**Question Three**

*You are having problems with finding enough time at combined board audit and risk committee meetings. How are you dealing with those issues?*

Question five in the survey was aimed at skill, timing and workload issues with combined board audit and risk management committees. While the findings suggested that overall these problems were not large, a number of survey respondents admitted to having some difficulty with this issue. The question was aimed at providing more information on the problem and the methods companies were adopting to address the problem.

**Question Four**

*Do you see any evidence of internal audit and risk management integrating across Australian companies – please explain?*

In response to survey questions seven, eight, nine, ten and eleven, respondents indicated various degrees of integration, mainly through short comments under their responses.

This interview question was designed to provide a fuller response to this issue and generally sought to explore the level of integration and what was driving that integration.

**Question Five**

*You have combined internal audit and risk management at the functional level. Can you comment on how this model aligns with the internal audit independence requirement?*
Survey question eleven required respondents to comment on how integrated risk and audit functions dealt with audit independence issues. The question was primarily aimed at finding out if the independence argument is a strongly held view. Also a secondary outcome was to understand the steps these integrated units adopted to maintain independence.

**Question Six**

*You do not have an internal audit function. Can you explain why no such function exists and how you cover assurance requirements for the board and board committees?*

Question twelve in the survey gave the respondents the option to respond that they had no internal audit function. Interviews were then required to establish why these companies failed to adopt internal audit and whether they had established a compensating agency control.

**Question Seven**

*You do not have a risk management committee. Can you explain how the ASX Principle Number Seven, to recognise and manage risk, is met?*

Question three in the survey gave respondents the option to declare that they have no risk committee at either board or management level. This interview question was aimed at establishing how risk management in those organisations is handled.

**Question Eight**

*Do you see internal audit as a subset of risk management – please explain?*

The survey responses revealed that risk management and internal audit were variously overseen by any one of a Company Secretary, CEO, CFO or a CRO. The question was designed to shed light on the structural hierarchy within Australian firms regarding risk and audit.
If internal audit was seen as a subset of risk management, a firm may place internal audit under a CRO, depending on independence concerns. If internal audit and risk management are seen as equally important pieces of the governance fabric, then a different structure may result.

This was a deliberately provocative question and was always asked as the last question. The question did indeed draw out some interesting responses and led to a number of new issues being highlighted.

3.7.6 Interview Process

All interviewees were sent an information statement when they received their initial survey and all had read an outline of the ethical considerations before agreeing to participate in the interviews. The survey instrument in the stage two surveys included a question on whether respondents would agree to a short interview. From the 102 valid survey responses, 52 respondents agreed to an interview, in writing, and provided their e-mail addresses for that purpose.

Interviews were conducted with three distinct categories of interviewee:

1. The survey respondents who agreed to an interview;

2. Four Big Four consulting firm partners. This was in addition to the S&P/ASX 200 survey respondents and was aimed at providing an industry overview that validated and supported the survey responses; and

3. Survey respondents who had a risk management function but no internal audit function. This unusual combination where a traditional internal audit is forgone, but risk management is present, was considered important to explore in the context of future directions.
Interviewing the Survey Respondents

In early August 2008, e-mails were sent to the first six interviewees, requesting a convenient time to conduct the interview and the best telephone number for that contact. Those e-mails explained that the interviews would be recorded. The e-mails also contained the questions for the interview. After three weeks passed without a reply to any of these six initial e-mails, two of the respondents were contacted by telephone. Each respondent advised that they were not prepared to participate if the interviews were recorded.

At that point, the author conceded that company secretaries of S&P/ASX 200 companies nearly all have a strong legal background. In the author’s experience, legal people have an ingrained tendency to discuss issues more freely if they are not recorded. Written responses or recorded interviews would require a legal person to spend much more time considering liability issues around each response. A decision was then made, in line with the Buchanan et al (1988) opportunistic approach, to delete the tape recording requirement from all future interviews.

The decision not to tape record the interviews meant that the author of the study had to record the interviews by taking notes. This was not a difficult decision as the researcher had spent over forty years working in a finance and commercial law environment. These roles involve hours at the negotiating table, taking copious notes of counterparty discussions, in a form suitable to be provided as evidence in subsequent court actions. Over this time the author had developed skills in the recording of verbal discussions.

In September 2008, e-mails were sent to the fifty-two survey respondents who had agreed to be interviewed. The e-mails asked for a time for the interview, a telephone number and provided the interview questions.
The e-mails also enclosed a draft organisational chart for each company, developed by the researcher using the desk-top information, survey responses and publically available governance information. The organisational charts outlined the governance structure at board, executive and functional levels for each individual organisation. As an introduction question, to establish rapport and trust (Cicourel, 1974, Dillman, 2007) the interviewees were asked to confirm these organisational charts as the first step in the interview process.

During October and November 2008 thirty five interviews were conducted with willing and very helpful interviewees. The remaining fifteen respondents had either left the organisation, refused to be interviewed once actual contact was made or just failed to respond to a number of repeated requests. The following table outlines the positions of the thirty five executives interviewed.

<table>
<thead>
<tr>
<th>Executive Position</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Secretary (COSEC)</td>
<td>12</td>
</tr>
<tr>
<td>Chief Risk Officer (CRO)</td>
<td>17</td>
</tr>
<tr>
<td>Chief Audit Executive (CAE)</td>
<td>3</td>
</tr>
<tr>
<td>Chief Finance Officer (CFO)</td>
<td>3</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>35</strong></td>
</tr>
</tbody>
</table>

*Figure 3.4 Thirty five executives interviewed in the first round of interviews during October and November 2008*

The interviews consisted of a thirty minute discussion on the eight questions noted above and the organisation chart, both of which were provided in advance. The researcher used a hands free phone and took notes of each interview.
Telephone interviews were chosen over face to face interviews because of cost and geographical considerations. Most of the company secretaries for the S&P/ASX 200 companies are located in Sydney and Melbourne, Australia. The author was located and working in Hobart, Tasmania, the island state of Australia. Substantial time off, air travel and costs would have been incurred if face to face interviews were conducted.

Adams, Khan and Raeside (2012) see telephone interviews as a valid research methodology and outline the problems with such interviews. The two main issues are a sense of impersonality and problems contacting people in the evenings when they are dining or relaxing. As the author was, at the time, a Chief Risk Officer of a large company, the impersonality issue was dissolved by talking to fellow executives with similar interests. The calls were also made during business hours, with the author taking annual leave to conduct the interviews.

Where significant quotes were made by the interviewee, care was taken to repeat the quote and record word for word. The written notes were transferred into an Excel spreadsheet under the following headings. These headings broadly align with the research questions discussed above.

<table>
<thead>
<tr>
<th>Organisational Structure</th>
<th>Maturity of ERM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit and Risk Synergies</td>
<td>Comments on Independence</td>
</tr>
<tr>
<td>Separate Risk Committee</td>
<td>Audit as a subset of Risk</td>
</tr>
<tr>
<td>Problems with Meeting Duration</td>
<td>No Risk Management</td>
</tr>
<tr>
<td>Comments on Integration</td>
<td>No Internal Audit</td>
</tr>
</tbody>
</table>

*Figure 3.5 Interview themes from first round interviews conducted over October and November 2008*
Interviewing the Big Four Risk Partners

To provide enhanced discussion and further triangulation on these themes, a senior risk management partner from each of PriceWaterhouseCoopers, Deloitte, KPMG and Ernst and Young (the Big Four) were interviewed. These interviewees could not speak for specific individual companies, but they provided a rich industry overview. The author was looking for validation and confirmation of the emerging themes.

Big Four partners are in demand and are difficult to book time with. A twenty minute interview would be unusually long. The author was faced with designing a very limited number of questions that captured the essence of each partner’s overview and allowed them to explore side issues if they had a particular point to make.

The author had recently completed the thirty five interviews with the survey respondents therefore the key issues were clear. The biggest issues unfolding were the roles of internal auditors versus risk managers, which neatly led into the integration between internal audit and risk management.

These two issues addressed organisational structure, audit and risk synergies, integration, maturity and audit independence.

To capture an industry perspective and keep within the limited time frame, the risk consultants were asked two simple questions:

1. Do you see any evidence of internal audit and risk management integrating across Australian companies? and

2. Do you see internal audit as a subset of risk management?

The first question encouraged a discussion on the roles of internal audit versus risk management and brought synergies, independence, role descriptions and organisational maturity into the discussions. The second question put the risk management and internal audit roles into perspective under a broader governance or agency perspective.
The second question was deliberately designed to be a little controversial, again to facilitate a richer discussion. The responses from the Big Four partners also validated the outcomes determined from the desk-top and survey analysis.

An interview of approximately twenty minutes duration was conducted with each of these risk consultants, all of whom provided a cross industry overview of the current situation. Notes were taken for each of these interviews and then transcribed into an excel spreadsheet. One of these partners provided an additional written follow up response to the interview questions by e-mail.

**Interviewing the “No Internal Audit” Companies**

Finally, the survey work in stage two indicated that fifteen of the one hundred and two companies that responded did not have an internal audit function. As a separate exercise, all fifteen were sent an e-mail and asked why they chose not to have an internal audit function. Five of those companies responded and interviews were then conducted with each of those companies, specifically asking why they chose not to have an internal audit. Those interviews are in addition to the thirty nine interviews conducted on wider risk matters and followed a similar interview procedure. The following table summarises the number of interviews conducted:

<table>
<thead>
<tr>
<th>Interviewee</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Survey respondents</td>
<td>35</td>
</tr>
<tr>
<td>Risk management partners in Big Four practices (additional to above)</td>
<td>4</td>
</tr>
<tr>
<td>Survey respondents without an internal audit function (additional to above)</td>
<td>5</td>
</tr>
<tr>
<td><strong>TOTAL INTERVIEWS</strong></td>
<td><strong>44</strong></td>
</tr>
</tbody>
</table>

*Figure 3.6  First, second and third round interviews with executives from the S&P/ASX 200 and Big Four*
The next section provides a summary of the data analysis that was undertaken on the desk-top, survey and interview data-sets.

3.8 DATA ANALYSIS

The data analysis can be treated in a logical order. Firstly, the quantitative work provided by the desk-top analysis and the survey is considered. Secondly, the surveys provided both quantitative and qualitative outcomes including a number of Likert scales which captured data on why different risk options are chosen. Finally the interviews provided a wealth of qualitative information.

As noted above, three data-sets resulted from the research. The first data-set related to the desk-top analysis of the annual reports of the Australian S&P/ASX 200 companies at 30 June 2007. The second data-set records the results of the survey from the same companies at the 30 June 2008. The third data-set records the responses to the interviews. For ease of distinction the first data-set will be called “the desk-top analysis data-set” and the second data-set, “the survey data-set”. Copies of a sample of each of the two quantitative data-sets are included as Appendices Two and Four.

3.8.1 Cleaning the Data-sets

Before commencing statistical analysis, Hair, Anderson, Tatham and Black (1998) suggest that the data should be examined for missing and outlying data and tested for the assumptions behind multivariate analysis.

After collection of the desk-top analysis and survey data-sets the data was “cleaned”, that is, checked for missing and outlying variables. Missing variables can be dealt with by restricting the analysis to the complete set, deleting the missing data-sets or imputing values by a number of statistical methods. There was little missing data found and in each case contact with the respondent provided the missing data.
3.8.2 Examining the Data-sets

The data-sets were then checked for normal distribution, linearity and correlation (Hair et al, 1998). Using the Statistical Package for Social Sciences (SPSS) both the desk-top and survey data-sets were screened using descriptive statistics. Since both data-sets included a mix of categorical and continuous variables, frequencies were derived for the categorical variables and descriptive statistics for the continuous variables.

In the desk-top analysis the only continuous variable REV (revenue in A$ million) produced the following descriptive table:

**REV (Revenue, in A$ million)**

<table>
<thead>
<tr>
<th>N</th>
<th>Min</th>
<th>Max</th>
<th>Mean</th>
<th>Std Dev</th>
<th>Skew</th>
</tr>
</thead>
<tbody>
<tr>
<td>REV</td>
<td>200</td>
<td>0</td>
<td>59341</td>
<td>3545</td>
<td>7286</td>
</tr>
</tbody>
</table>

*Figure 3.7 Descriptive information for revenue in the S&P/ASX 200 in the desk-top analysis*

In the desk-top analysis the two categorical variable GICS (industry classification) and ADR (board committee set-up) produced the following frequency table:
The table below shows the GICS classification frequency and percentage for the S&P/ASX 200:

<table>
<thead>
<tr>
<th>GICS Classification</th>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 – Energy</td>
<td>15</td>
<td>7.5</td>
</tr>
<tr>
<td>15 – Materials</td>
<td>39</td>
<td>19.4</td>
</tr>
<tr>
<td>20 – Industrial</td>
<td>31</td>
<td>15.4</td>
</tr>
<tr>
<td>25 – Consumer Discretionary</td>
<td>26</td>
<td>12.9</td>
</tr>
<tr>
<td>30 – Consumer Staples</td>
<td>9</td>
<td>4.5</td>
</tr>
<tr>
<td>35 – Health</td>
<td>9</td>
<td>4.5</td>
</tr>
<tr>
<td>40 - Financial</td>
<td>53</td>
<td>26.3</td>
</tr>
<tr>
<td>45 – Information Technology</td>
<td>3</td>
<td>1.5</td>
</tr>
<tr>
<td>50 – Telecoms</td>
<td>4</td>
<td>2.0</td>
</tr>
<tr>
<td>55 – Utilities</td>
<td>12</td>
<td>6.0</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>200</strong></td>
<td><strong>100.0</strong></td>
</tr>
</tbody>
</table>

**Figure 3.8  Descriptive information by GICS for the S&P/ASX 200 in the desk-top analysis**

Figure 3.8 showed that for GICS classification 45 and GICS 50, the frequency is very small, 3 and 4 companies respectively. Care will need to be taken with the findings from such small samples.

The table below shows the board committee arrangement frequency and percentage for the S&P/ASX 200:

<table>
<thead>
<tr>
<th>Board Committee Arrangement</th>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 – No board risk committee</td>
<td>21</td>
<td>10.4</td>
</tr>
<tr>
<td>1 – Separate board risk committee</td>
<td>34</td>
<td>16.9</td>
</tr>
<tr>
<td>2 – Board risk committee combined with audit committee</td>
<td>145</td>
<td>72.6</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>200</strong></td>
<td><strong>100.0</strong></td>
</tr>
</tbody>
</table>

**Figure 3.9  Descriptive information on ADR for the S&P/ASX 200 in the desk-top analysis**
In the survey analysis the continuous variables REV (revenue in A$ million) and YRS (years since incorporation) produced the following descriptive tables.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>YRS</td>
<td>102</td>
<td>1</td>
<td>54</td>
<td>16.73</td>
<td>13.042</td>
<td>1.063</td>
</tr>
<tr>
<td>REV</td>
<td>102</td>
<td>0</td>
<td>59341</td>
<td>4480</td>
<td>9071</td>
<td>4.139</td>
</tr>
</tbody>
</table>

**Figure 3.10**  
*REV (Revenue in A$ million) and YRS (Years since incorporation) for S&P/ASX 200 companies from the survey analysis*

Frequency analysis for the categorical variables in the survey data-set included, GICS (industry classification), ERM (maturity of ERM), ADR (board committee set-up), EXO (executive officer), FUN (functional set-up) and IAU (internal audit set-up). That frequency analysis is included as Appendix Ten.

### 3.8.3 Data Relationships

Hair et al (1998) recommend the completion of correlation matrices for the data-sets, to determine whether any relationships exist between the variables. Figures 3.10 and 3.11 below, outline the variables for each data-set and classify which variables are continuous and which are categorical. Continuous variables are numeric and can be ordered sequentially, for example, revenue and years since incorporation are continuous. Categorical variables cannot be ordered sequentially or differentiated from one another using common mathematical methods. Examples of categorical variables would include GICS, type of board risk committee and executive oversight of risk, all of which are non-numeric categories.
<table>
<thead>
<tr>
<th>Desk-top Variable</th>
<th>Data-set</th>
<th>Type</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIGS</td>
<td></td>
<td>Categorical</td>
<td>Between GICS 10 (Energy) and GICs 55 (Utilities) in discrete groups</td>
</tr>
<tr>
<td>REV</td>
<td></td>
<td>Continuous</td>
<td>Between 0 and A$ 60,000m</td>
</tr>
<tr>
<td>ADR</td>
<td></td>
<td>Categorical</td>
<td>Can only be a 1, 2 or 3.</td>
</tr>
</tbody>
</table>

*Figure 3.11 Categories of variables for desk-top analysis data-set*
<table>
<thead>
<tr>
<th>Survey Variable</th>
<th>Data-set</th>
<th>Type</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADR</td>
<td>Categorical</td>
<td>Can only be a 1, 2 or 3.</td>
<td></td>
</tr>
<tr>
<td>REV</td>
<td>Continuous</td>
<td>Between 0 and A$ 60,000m</td>
<td></td>
</tr>
<tr>
<td>YRS</td>
<td>Continuous</td>
<td>Between 1900 and 2008</td>
<td></td>
</tr>
<tr>
<td>GICS</td>
<td>Categorical</td>
<td>Between GICS 10 (Energy) and GICs 55 (Utilities) in discrete groups</td>
<td></td>
</tr>
<tr>
<td>ERM</td>
<td>Categorical</td>
<td>Can only take discrete values from 1 to 5</td>
<td></td>
</tr>
<tr>
<td>EXO</td>
<td>Categorical</td>
<td>Can only take discrete values from 1 to 7</td>
<td></td>
</tr>
<tr>
<td>FUN</td>
<td>Categorical</td>
<td>Can only take discrete values from</td>
<td></td>
</tr>
<tr>
<td>IAU</td>
<td>Categorical</td>
<td>Can only take discrete values from</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 3.12 Categories of variables for the survey analysis data-set**

The majority of the above variables are categorical. When considering the relationships in the above tables, the independent variable ADR (audit and risk arrangement at board level) is categorical.

Also most of the dependent variables are categorical. Standard least squares regression and multivariate analysis are not normally suited to categorical variables: “measuring the strength of an association between two categorical variables turns out to be a non-trivial task” (Wilcox, 2009, p 265).
To measure the relationship between categorical variables requires specific statistical tests, such as Chi Square and tests of proportions. The use of a correlation matrix to test the data was rejected due to the categorical nature of the variables.

Given the discrete nature of the data-sets and the high proportion of categorical variables graphical and descriptive analysis was chosen over regression analysis.

### 3.8.4 Graphical and Descriptive Analysis

Leung et al (2004) use a combination of pie charts, histograms and tables to analyse and present the facts and opinions gained from their survey. This type of analysis, using graphs and tables is also suitable for basic descriptive analysis such as checking for normal distribution, linearity and correlation. These tools can also be used to clean data and fill in missing variables. In contrast, more complex mathematics such as linear regression, probit and logit were used to explore the relationships in the Beasley et al (2005), Kleffner et al (2003) and Carey et al (2006) studies noted earlier.

In the findings chapter the results from a simple descriptive examination of the data are outlined. That descriptive analysis primarily used observations from both the data-sets. Both the desktop and survey data-set outcomes, and particularly the Likert scales, were suited to graphical and descriptive analysis. The graphs, pie-charts, histograms and tables provided insight into the risk management structure in Australia’s leading companies. The interviews then shed light on the reasons for adopting those structures and what is driving changes within the governance arena.

### 3.8.5 Analysing the Interviews

Interviews were conducted at three levels:
1. with thirty five executives from the S&P/ASX 200 companies;

d2. with five S&P/ASX 200 executives that had no internal audit functions; and

3. with four risk management partners from Big Four consulting practices.

When analysing interviews, King and Horrocks (2010) discuss two approaches, one focusing on language and the other on content. Basing the analysis on language is used to ascertain how language is used in social interactions and how the story is told. This method is useful in the social constructionist tradition (Burr, 2003) and includes discourse and narrative analysis. The context approach, which focuses on the experiences of those interviewed, from their own perspective, (Langridge, 2007) is used in this study. An experienced based methodology would better uncover the drivers and behaviours that sit behind different management structures.

Dey (1993) takes the reader through a wide variety of techniques, including ethnographic analysis and semiotics all of which appear to have evolved from philosophy and human science. Sue Jones in Walker (1993, p.58) outlines a much more understandable and practical approach whereby transcripts are analysed into logical groupings, cognitive mapping, that shed light on the research problem. Walker also adds that “pulling statements from the interview” and making lists of “propositions or relationships” help complete this picture.

Both Fraser and Henry (2007) and Leung et al (2004) use the Walker approach. The Leung et al analysis of interviews includes the following quotations:
• “Findings from the interviews are discussed by evaluating common themes”;

• “The prevailing view of all interviewees was that non-executive directors made a significant contribution to the governance process”;

• “At least one organisation had a formal training process for inducting audit committee members”; and

• “Another CAE gave an example of using the Audit Committee as a forum of last resort on a risk issue”.

Rather than trying to generalise comments back to the whole population, the quotations underpin and support possible interpretations on the research problem.

Miles and Huberman (1994) divide data analysis into four components: data collection; data display; data reduction; and drawing conclusions. These categories helped with the following data analysis.

**Thematic Analysis**

Thematic analysis is about identifying common themes from the interviews. Braun and Clarke (2006) see themes as patterns in the data that say something interesting about research. King and Horrocks (2010) provide the following definition:

> Themes are recurrent and distinctive features of participant’s accounts, characterizing particular perceptions, and/or experiences, which the researcher sees as relevant to the research question.

Since the research focuses on the drivers behind governance structures the themes outlined by the executive managers interviewed are of interest and relevant. An often repeated theme may reveal a solid rationale for a chosen management structure.
For example, when asked about the synergies between internal audit and risk management, several interviewees talked about a “Circular Flow” theme.

The author chose to use thematic analysis, or the analysis of underlying themes as outlined by Braun and Clarke (2006) and discussed in King and Horrocks (2010). This approach aligns closely with the Walker (1993) methodology as noted above. Themes or distinct repetitive patterns were drawn from the interviews using a structured approach. The themes were arranged in a hierarchical relationship as suggested by Langridge (2004) and Braun and Clarke (2006).

Langridge breaks thematic analysis into three distinct stages:

1. Stage One – descriptive coding;
2. Stage Two – interpretive coding; and

Firstly, the transcript data that was most likely to help address the research question is identified. In this study, the data collection phase resulted in ten categories, each broadly aligning to a research question. These categories are outlined below and effectively comprise the descriptive coding phase of the research as discussed by Langridge (2004). Descriptive codes are labelled using short phrases as suggested by Langridge.

For each descriptive coding the number of interviewee responses is noted:
<table>
<thead>
<tr>
<th>No</th>
<th>Descriptive Coding</th>
<th>Number of Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>Organisational Structure</td>
<td>35</td>
</tr>
<tr>
<td>02</td>
<td>Maturity of ERM</td>
<td>28</td>
</tr>
<tr>
<td>03</td>
<td>Audit and Risk Synergies</td>
<td>33</td>
</tr>
<tr>
<td>04</td>
<td>Comments on Independence</td>
<td>18</td>
</tr>
<tr>
<td>05</td>
<td>Separate Risk Committee</td>
<td>22</td>
</tr>
<tr>
<td>06</td>
<td>Audit as a Sub-set of Risk</td>
<td>22</td>
</tr>
<tr>
<td>07</td>
<td>Problems with Meeting Duration</td>
<td>18</td>
</tr>
<tr>
<td>08</td>
<td>No Risk Management</td>
<td>3</td>
</tr>
<tr>
<td>09</td>
<td>Comments on Integration</td>
<td>29</td>
</tr>
<tr>
<td>10</td>
<td>No Internal Audit</td>
<td>5</td>
</tr>
</tbody>
</table>

**Figure 3.13  Descriptive coding from interviews with thirty five S&P/ASX 200 executives**

Miles and Huberman (1994) contend that: “valid analysis is immensely aided by data displays that are focused enough to permit viewing the full data-set in one location”. This type of physical display aligns with the mind mapping concepts discussed by Langridge (2004) and Braun and Clarke (2007).

The researcher arranged ten A3 sheets of paper from Excel, one for each heading or descriptive coding (see figure above), with up to thirty five responses on each sheet. The sheets were then enlarged to A2 and attached to a wall, to allow for logical grouping, data reduction and analysis.

The next stage undertaken is termed data reduction by Miles & Huberman (1994) or interpretive coding by Langridge (2007). Each descriptive code was reviewed for interpretation of the interviewee’s responses. A good example of this approach is found within the descriptive coding: 03 - Audit and Risk Synergies.
Within that category, the thirty three respondent transcripts could be coded into eight clear interpretations:

<table>
<thead>
<tr>
<th>Descriptive Code – Audit and Risk Synergy (03)</th>
<th>Interpretive Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>03-01</td>
<td>Circular flow</td>
</tr>
<tr>
<td>03-02</td>
<td>Three lines of defence</td>
</tr>
<tr>
<td>03-03</td>
<td>Annual accounts are a risk scorecard</td>
</tr>
<tr>
<td>03-04</td>
<td>Risk register</td>
</tr>
<tr>
<td>03-05</td>
<td>Risk and internal control</td>
</tr>
<tr>
<td>03-06</td>
<td>Continual improvement</td>
</tr>
<tr>
<td>03-07</td>
<td>All governance</td>
</tr>
<tr>
<td>03-08</td>
<td>All care no responsibility</td>
</tr>
</tbody>
</table>

*Figure 3.14 Interpretive coding for interview question on audit and risk synergy*

For the descriptive coding above (03 – Audit and Risk Synergy) the author had one A2 wall mounted sheet that showed the descriptive code, with eight interpretive sub-codes, which were the grouping of respondent's transcripts. A copy of the recording of this descriptive code is attached as Appendix Eleven. That appendix shows the transcript of the actual interviewee responses. This process was repeated for all ten interpretive categories noted above in figure 3.12.

The final stage of analysis, which Miles and Huberman (1994) term drawing conclusions, was to define the overarching themes for each descriptive code, as outlined by Langridge (2007). In the above example the eight interpretive codes were reduced to four themes by listing the more frequent and overarching themes. The less common, more marginal themes were able to be utilised under other interpretive codes. The four resulting underlying themes are:
1. circular flow;
2. three lines of defence;
3. annual accounts are scorecard for risk management; and
4. similarity between internal audit and risk management.

King and Horrocks (2010) suggest that between two and five overarching themes can be identified for each descriptive code.

A similar process was undertaken for all ten descriptive codes depicted in Figure 3.12. At this stage, as outlined by King and Horrocks (2010) the theoretical ideas and applied concerns underlying the study were also used to help identify the overarching themes. The stages of developing and organising the descriptive codes, the interpretive codes and the underlying themes are recorded on the A2 wall sheets to provide auditability.

Advanced computer software analysis of the interview data was not required. According to Sue Jones in Walker (1993) doing this analysis manually, with limited assistance from Microsoft Word or Excel helps the researcher better understand the issues in the context of the interviewee’s responses. The possibility of using Nvivo, Nud*ist or XSight interpretive analysis software was considered but rejected because the outputs of thirty five interviews were able to be handled in Excel spreadsheets.

The themes or logical groupings drawn from the interviews were then used to validate, support and add detail to the desk-top analysis and survey findings. These themes, often supported by quotations, were used as supporting narrative when the desk-top analysis and survey conclusions were summarised in the next chapter. Also, as a result of the above interviews, four models for governance oversight of risk management emerged. The models are based on the organisational structures (descriptive coding 01) provided by each interview respondent. The models also draw on aspects of the other descriptive coding: integration, independence, maturity, audit relationship to risk and existence of internal audit.
The models all reflect different levels of integration between risk management and internal audit and appear to be based on different levels of management maturity and with some historical legacy issues.

Finally, the Excel and Word documents, designed to handle the outcomes from the desk-top analysis, survey and interview analysis were all arranged as a data management system. The author, as a former CAE, often uses such systems to handle the data flowing from complex or large audits. This allows the grouping, sorting and extraction of data, without loss of integrity.

As an example of this:

1. the findings from the desk-top analysis of the S&P/ASX 200 was set up as a relational data-base, thereby allowing sorting and grouping;
2. the Likert scales were also set up as a relational data-base, thereby allowing sorting and grouping;
3. the responses, and comments, from the survey, were set up as a relational data-base; and
4. the interview responses were arranged under each descriptive code, in logical groupings, with unique numbers for each subset.

The final section looks at a compensating validation procedure, given that the interviews were not taped.

### 3.9 RESEARCH VALIDATION

Before the findings are discussed, it is important to consider validation of the interpretation of the survey and the interviews conducted. The interviews were not taped. It was therefore necessary to develop mechanisms to validate the interview findings. Such validation helps to ensure that the interviewer has addressed reliability and interviewer bias issues. It also helps confirm that the data analysis, which led to common groupings, is reasonable.
As noted earlier, the survey question design was validated by a comprehensive quality assurance process.

The overall validation consisted of a three stage process:

1. A journal article written by the author, see Appendix Six;
2. Interviews with four Big Four risk management partners; and
3. Comments back on the draft abstract, see Appendix Twelve.

The draft abstract was sent to the interviewees for validation, see Figure 3.14 below.

**Journal Article**

In March 2008 the author published an article on the role of board audit committees in risk management, see Appendix Six. In that article the author outlined the early desk-top results on the percentage of S&P/ASX 200 companies with:

1. a combined board audit and risk committee;
2. a separate board risk committee; and
3. no board risk committee.

The article also discussed the skill levels required by audit committee members, the reasons for having no risk presence at board level, internal audit and risk management integration, and a view of ERM from corporate Australia.

The article was designed to inform the Australian risk management community on the study, and to seek comments from interested parties on the direction of the research. A copy of the article was sent to all S&P/ASX 200 identified executives as part of the survey pre-notice letter in May 2008.
The author received no negative comments on the future direction of the research. As a result of the article, the author was contacted by KPMG and Deloitte both of whom requested access to the final study and the opportunity to work with the author on aspects of the study. The author was also contacted by four other organisations, all of whom were considering combining their internal audit and risk management functions. The author then advised those organisations on different aspects of audit and risk integration.

Interviews with Big Four Risk Partners

As noted above, the author also conducted interviews with a risk management partner from each of the Big Four accounting practices. These interviews were aimed at providing an industry wide perspective on the research issues. These interviews also served to provide validation for the research.

In general the comments from these Big Four partners confirm that integration of audit and risk is occurring (albeit at different levels) there is competition between the CFO’s and CRO’s and risk management is becoming a large issue for board consideration. The following quotes from risk partners support the direction of the study.

Risk Partner One

*The cross-over and interdependency between audit and risk is where the internal audit program requires risk based skills to unpick or study the exposure in quantitative terms or operational terms in areas outside of finance/conventional educational base. They are co-dependent in my view.*
Risk Partner Two

There are varying degrees of integration across corporate Australia. Many larger, older more traditional organisations still keep internal audit and risk management separated. The banks are making progress with integration, often having audit reporting to the CRO. Where separation is apparent, independence and communication play a role, as does competition between executives.

Risk Partner Three

On integration there is evidence at the oversight at board level but not so strong at operational level. Risk managers are often a different group of people. The three lines of defence model is starting to take hold, hence more integration. Integration brings the CFO into competition with the CRO and that may pose a threat to the integrated model. Board committees are recognising more and more that risk is more about the risk return trade off.

Risk Partner Four

There is evidence of integration at the functional level with some internal auditors seeking greater skill in risk based sciences, but perhaps in real terms there is still separation at the intellectual level. For internal auditors to be more successful they may need to address some blind-spots or areas of discomfort in looking forward and addressing the forecast environment. This is not to suggest that internal auditors are incapable of discussing forecasts and the future, it is more that they show an inclination for embedding themselves in proving the past. Functional integration has been popular with the creation of the so-called "chief risk office" portfolio. We have observed how this functional set up works or doesn't, and observe again that behavioural bias ends up setting the direction of such functions.
The risk people want to get involved in strategy and decision making while the audit people would like to but are not sure how to claim legitimacy in such internal activities.

Interviewee Comments on Abstract

Finally, an abstract, that summarised the findings from the desk-top analysis, the findings from the survey and in particular the interview findings, was developed. That abstract is included as Appendix Twelve. The abstract was sent to the thirty nine interviewees, including the Big Four partners interviewed, with a request for them to comment on the findings. In particular, they were asked to provide comments on any inconsistency or anything that they found were at odds with their understanding. This approach was used by Covaleski and Dirsmith (1988) to ensure that they had accurately portrayed the experiences of University budget participants in their study.

Twenty seven of the original thirty nine interviewees responded with comments on the abstract. All comments were constructive and supportive and no interviewee had a disagreement with any finding. Some examples of the comments received are included in the following table:
Overall, the three stages of validation, as outlined above, confirm that the interviewees are comfortable with the results, find them to be what they expected and had no major suggestions for change.

The next chapter presents the findings from the above research.
CHAPTER FOUR - FINDINGS

4.1 INTRODUCTION

In this chapter the findings from the desk-top analysis, the survey and the interviews conducted with executives from the S&P/ASX 200 leading Australian companies are presented.

The primary research aim was to examine the organisational structure that is used to facilitate risk management in leading Australian companies, including an analysis of the tensions and strengths of integrating risk management with internal audit.

In order to fulfil this aim, three research objectives had been identified:

1. To investigate the structure of risk management at the board, executive and functional levels in Australian companies. This included the reasons for audit committee involvement in risk management and the role of separate board risk committees. The skill, timing and workload aspects of bringing risk management into the audit committee was also investigated as well as the placement of the CRO;

2. To establish the levels of integration between internal audit and risk management in leading Australian companies. This includes the extent to which the internal audit profession independence requirement is preventing such integration; and

3. To identify which models are being used to govern risk management in the S&P/ASX 200 Australian companies. That also included the arrangements for both internal audit and risk management in those models.

This chapter draws the theories, the debates, the gaps and the research methodologies together to develop answers to the primary and related research questions.
This chapter commences with a discussion of the findings from the desk-top analysis and the survey. That work clearly shows what risk management structures and arrangements are present in leading Australian companies.

The desk-top and survey analyses also indicate why these particular structures have been chosen. The chapter then moves into a discussion on the synergies between internal audit and risk management, a strong theme throughout this work. The relationship between that synergy and knowledge management (KM) is developed and the importance of the synergy in the integration between internal audit and risk management is outlined.

The outcomes of interviews with thirty nine risk management executives are then discussed. The interviews, which draw heavily on the idea of synergy, flesh out many of the concepts raised in the survey and provide a level of subtlety and richness that enhances those survey responses. Finally, drawing on the desk-top analysis, survey and interviews, a set of models for the management of risk in leading Australian companies is developed.

4.2 AT BOARD COMMITTEE LEVEL

In this section the governance of risk management at the board committee level for S&P/ASX 200 companies is discussed. The first research objective for this study was to investigate the structure of risk management at the board, executive and functional levels in Australian companies.

KMPG (2005) and Subramaniam et al (2009) found that, in Australia, risk is managed through the board audit committee in 70% and 75% of companies respectively. However, the reasons for adopting that model were not investigated in those studies.

The desk-top and survey analyses found that three types of board risk committee structure exist:
1. a combined board audit and risk committee;
2. a separate board risk committee; and in some cases
3. no board risk committee.

The fact that some leading Australian companies do not support a board risk committee is a new finding that has not been previously explored in the literature.

Figure 4.1 below, outlines the findings from the desk-top analysis of S&P/ASX 200 companies. These results are for the entire population of 200 companies that were listed by the ASX on 30 June 2007. One hundred and forty six of these Australian companies, or 73%, have combined their audit and risk committee into a single board committee. This finding aligns with the previously cited KPMG (2005) and Subramaniam et al (2009) studies.

![Figure 4.1](image)

**Figure 4.1** Board risk committee arrangements in the S&P/ASX 200 companies. A sample of 102 observations from a population of 200 which at the 95% confidence level gives a confidence interval of +/- 7%
Figure 4.1 also highlights that 17%, or 34 Australian companies have a separate board risk management committee to oversee risk management activities.

Twenty companies comprising 10% of the population have indicated in their annual reports that they have no risk management committee at board level.

To validate these findings, the desk-top analysis results and the results from the survey were triangulated. The following table outlines these comparisons.

<table>
<thead>
<tr>
<th>Category at Board Level</th>
<th>Combined board audit and risk committee</th>
<th>Separate board risk committee</th>
<th>No board risk committee</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desk-top Analysis (population 200)</td>
<td>73%</td>
<td>17%</td>
<td>10%</td>
</tr>
<tr>
<td>Survey responses (102 responses)</td>
<td>67%</td>
<td>24%</td>
<td>8%</td>
</tr>
</tbody>
</table>

**Figure 4.2 Triangulation of desk-top analysis results with survey results**

To determine whether the values of the survey sample in Figure 4.2 are statistically significant with regard to the population, a Chi Square test was completed, using the following calculation:

```
<table>
<thead>
<tr>
<th>Category at Board Level</th>
<th>Sample % (Oi)</th>
<th>Pop % (Ei)</th>
<th>Oi-Ei</th>
<th>Oi-Ei Squared</th>
<th>Chi Square</th>
</tr>
</thead>
<tbody>
<tr>
<td>Combined</td>
<td>68</td>
<td>75</td>
<td>-7</td>
<td>49</td>
<td>0.653</td>
</tr>
<tr>
<td>Separate</td>
<td>24</td>
<td>17</td>
<td>+7</td>
<td>49</td>
<td>2.882</td>
</tr>
<tr>
<td>No Committee</td>
<td>10</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>N</td>
<td>102</td>
<td>102</td>
<td>0</td>
<td></td>
<td>3.536</td>
</tr>
</tbody>
</table>
```

**Figure 4.3 Chi Square statistical significance results for Figure 4.2**
From a statistical table (Hanneman, Kposowa and Riddle, 2012) at alpha = 0.05, and 2 degrees of freedom, the critical value of $X^2$ squared is 5.991. Since the Chi Square value of 3.536 < 5.991, the null hypothesis cannot be rejected therefore the sample is statistically representative of the population at the 0.05 level of significance.

The desk-top analysis provided data from the entire population of all S&P/ASX 200 companies and the survey data came from 102 respondents or 59% percent of the population. In general, the results support one another.

Triangulation also serves an added purpose. Armstrong and Overton (1977) outline the problem of non-response bias in mail surveys. The fact that the desk-top analysis and the survey results are closely aligned helps indicate that the survey does not suffer from strong non-response bias.

Prior research, such as that completed by Subramaniam et al (2009), Ruigrok et al (2006) and Benz and Frey, (2007), linked factors such as company size, revenues and board committee structure to agency theory. The creation of board committees as an agency response was linked to the size, industry classification and other company characteristics. The average revenue for the desk-top analysis population of S&P/ASX 200 companies was $3,443 million. The average revenue for those companies having a combined board audit and risk committee was $3,617 million. These average revenues suggest that combined audit and risk committees are not skewed to larger or smaller companies within the S&P/ASX 200.

Subramaniam (2009) found that the existence of risk management committees, either executive, standalone or combined with the audit committee increased with the organisations size. The relationship between organisation size and type of risk management committee is further explored in later sections of this Chapter.
In summary, the desk-top analysis supported by the survey shows that 73% of S&P/ASX 200 Australian companies have a combined board audit and risk committee. Seventeen percent of S&P/ASX 200 companies have a separate board risk committee and 10% have no board risk committee.

In the next section, the reasons for integration between audit and risk at the board committee level are discussed.

4.3 BOARD AUDIT AND RISK COMMITTEES

Seventy three percent of S&P/ASX 200 companies have a combined board audit and risk committee.

Australia may be a follower with respect to board audit and risk committees. The United Kingdom Turnbull report first raised the issue of board risk committees in 1999. This was closely followed by COSO-ERM in the United States in 2002. Australia issued its ASX Principles in 2003, followed by the Australian Risk Management Standard AUS/NZS 4360:2004. All of these regulators have advocated a strong risk management presence at board level.

This timeline supports an institutional theory view, that Australian companies are following their international peers to combine audit and risk management at board committee level. Australian companies, when faced with this new risk management technology, ambiguous goals and uncertainty following corporate collapses, would imitate the overseas experience. These uncertain factors, as noted by DiMaggio and Powell, (1983) may be driving this mimetic isomorphism.

Question four of the survey (see Appendix Three) asked respondents to rank a number of factors as possible reasons for combining board audit and risk committees. The factors were determined from pilot interviews. Each factor was scored on a Likert scale of one to five, with one being of no importance and five being very important.
The following graph outlines the average scores for the survey responses:

![Graph showing average scores for combining board audit and risk committees]

**Figure 4.4 Reasons for combining board audit and risk committees**

An average score of two point five indicates the point of indifference, scores above two point five indicate that the rationale becomes more important and scores below two point five indicate lesser importance. On that basis it can be seen that convenience, the adoption of what is considered the industry standard and synergy, as outlined in the research questions, are important factors in combining audit and risk at the board committee level. Surprisingly, cost is the lowest on the list and therefore not a significant driver for combined committees. The absence of cost as a motivation could provide an avenue for future research.

By far the most important factor, or reason for combining board committees, is the synergy between audit and risk. Respondents to the surveys indicated that the synergy between audit and risk is the most important factor in the decision to integrate these functions into a single board committee.
As the research progressed, the importance of this synergy between audit and risk became clear. Synergy underpins many of the structures uncovered and is also a prime consideration in the integration of internal audit and risk management. Therefore the following section of this chapter has been devoted to the concept of synergy.

4.4 THE SYNERGIES BETWEEN INTERNAL AUDIT AND RISK MANAGEMENT

Earlier in this chapter, section 4.3 outlined that respondents to the survey indicated that the synergy between internal audit and risk management underpins the decision to adopt a combined board audit and risk committee. This section provides more detail on the concept of synergy, and uses the responses from surveys and interviews to explain the prevailing perception of such synergy.

In Chapter Two, the concept of synergy was raised in a number of contexts. Looking for overlap between internal audit and risk management, possible synergies were identified as:

- both internal control and risk management are a management responsibility, facilitated by the internal auditor or risk manager, (McNamee, 1997);
- the objectives of both internal audit and risk management overlap, (Phillips, 2008);
- internal audit and risk management are both systems of internal control, (Spira and Page, 2002); and
- the “Three Lines of Defence” model, integrates internal audit with risk management in an overall defence model, (Micallef, 2008).

Comments provided by the survey respondents in the comments section of survey question four (see Appendix Three) shed light on what defines this synergy between audit and risk.
The interviews with thirty five companies and four risk consultants added extra colour. The respondents felt that synergy could be explained in terms of:

1. what they termed the circular relationship between risk management and internal audit;
2. the relationship between risk and audit in the “three lines of defence model”;
3. the relationship between risk management and the annual accounts;
4. the similarities between internal audit and risk management; and
5. the prevention of “turf wars” between different board committees.

The following sections outline the respondent’s views on the definition of synergy and why this relationship helps explain the integration of internal audit and risk management. Where possible, the actual comments from participants are used to highlight these issues.

4.4.1 Circular Flow

The synergy between internal audit and risk management, according to the comments in the survey and supported by interviews was explained by some respondents as what is termed the audit and risk “circular flow”. The concept of this circular flow, as portrayed in Figure 4.4 below, was raised by many participants and the actual wording “circular flow” was suggested by two of the executives involved in the interview sections of the research.
Commencing with the strategic planning process, management and in particular the risk managers assess the risks to the organisation. These risks are entered into the risk register and become the risk profile. Management then takes those identified risks and design mitigations to address the risks.

These mitigations may be in the form of actions, processes, internal controls, risk transfer (such as insurance and hedging) or even strategies to accept or avoid risk. In essence, these actions or mitigations become the major activities, the work programs and the focus of management for the next period of time.

The internal auditors’ then use the above risk profile, generated by the risk managers, to design their audit plan for the coming period. The audit plan, prioritised by risk likelihood and consequence, leads to reviews of the action plans, mitigations and internal controls adopted by management. Where these management activities are found to be inadequate or lacking a new risk arises. The internal auditors then work with management to improve the internal controls where such risks are identified. This process is an accepted tenant of both modern internal audit (Moeller, 2004) and contemporary risk management (ISO 31000:2009).

As is portrayed in figure 4.4 below, this process takes on a circular flow. An executive from a financial services company explained:

There is a circular flow. The internal auditors use the outcomes from risk analysis to focus their annual plan on the high risk areas. The risk managers use the outcomes from audit activity to identify areas of higher risk, then mitigate accordingly. (CRO from a GICS 40 company)

That cycle comprises the circular flow. Risks are identified and mitigations are assigned. The audit plan is designed around these risks, mitigations are reviewed and new risks are identified by the auditors. The new risks are fed back into the cycle.
An energy company executive supported this circular flow:

There is a natural flow of synergy. The outcomes of strategic and operational risk management drive the internal audit plans. The outcome of the internal audit work finds more risks and tells us how we are going on risk management, both of which feed back into risk management. (COSEC from a GICS 10 company)

An executive from an industrial company explained the concept of the circular flow in a little more detail:

We see synergies between audit work and risk management. Both are governance components of management. The annual audit plan is derived from a thorough understanding of company-wide risks. Alternatively, the audit work uncovers additional risks or problems with mitigations that the audit committee needs to feed into overall risk management. (CAE from a GICS 20 company)

In this circular flow the risk register, owned by the risk managers, becomes a tool of audit.
A prioritised risk register helps the auditors identify the more significant risks and the controls, or mitigations that management use to reduce the risks.

Two executives, one from a materials company and one from an energy producer both explained the importance of the risk register:

*The electronic risk register can also be a tool for internal audit, used to select internal controls for conducting their validation work.* (CRO from a GICS 15 company)

*Over recent years internal audit has been able to become more efficient and more focused by using the full risk register to determine where to direct audit activities.* (CAE from a GICS 10 company)

The concept of a circular flow also relies heavily on a risk based internal audit approach. Such an approach is good internal audit practice and was identified by McNamee and Selim (1998) as discussed in Chapter Two. An executive from a financial company outlined this process:

*We have an orthodox charter for the audit, risk and compliance committee. The committee looks at the top twenty operational risk issues. The committee requests that the outsourced internal audit function provide a better understanding of each risk, and progress on mitigations. In this context, risk is the antenna and internal audit helps with the solution.* (CRO from a GICS 40 company)

The relationship that sees the risk managers identifying risks and the internal auditors testing and then adding new risks, fits with the Leung et al (2004) finding in Chapter Two where:

*Forty eight percent of CAE’s strongly agreed that internal audit should bring a systematic and disciplined approach to evaluating and improving the effectiveness of risk management.*
In a number of the organisations interviewed, the circular flow model is taken to the next logical step, perhaps the next paradigm shift, identified by McNamee and Selim (1998), where internal audit and risk management functions become integrated.

The following is a comment from a finance company executive whose company does not have an internal audit function. The risk managers have taken on the role of de-facto internal auditors:

*We (the risk managers) complete the risk reviews and keep abreast of internal controls. When we find a problem or issue, or a mitigation is required, we allocate the solving of that problem to management, a team member or an external contractor if specialised expertise is required. We see this process of risk as the initiator and de-facto audit as the fixer as a process of continual improvement.* (CRO from a GICS 40 company)

This blending sees both internal audit and risk management identifying risks and both functions recommending mitigations. It is not a huge leap to see a more combined role for these functions.

It is clear from the above that having both risk management and internal audit reporting through to a single board committee facilitates this circular flow. Having a separate board risk committee would break this flow, especially within an organisation that has adopted a silo approach. To again quote Connelly (2009) from Chapter Two:

*As a board we realised that we could not separate risk from audit and do our job. How can you account for assets and set up reserves without assessing risk?* (Connelly, 2009)

Having audit matters and risk matters considered in the same forum will allow knowledge management (KM) to help transfer tacit to explicit knowledge.

This integration is also supported by a consumer discretionary company executive, who felt that:
Risk and control are considered to be interdependent. By combining these functions at board level it ensures discussion at the same forum. (CRO from a GICS 25 company)

Combined board audit and risk committees can oversee the risk assessment process and outcomes and approve the risk based audit plan. The combined board committee can then review the audit outcomes, which relate to the management’s commitment and success in mitigation of risks. Finally the board audit and risk committee can enforce any additional controls or mitigations identified by the auditors. From an agency perspective, this lowers the agency cost of having two separate board committees. Having risk management and internal audit planned, monitored and controlled by one committee would both keep down agency costs and allow knowledge to be shared with a small but effective group.

This circular flow synergy is an example of KM being used for competitive advantage. Grant (1996) argues that firms exist to create the conditions in which specialists can integrate their knowledge. Combining internal audit and risk management in a single board audit committee would ensure the integration of knowledge. Having the auditors and risk managers integrated and working together would facilitate the transfer of tacit know-how into explicit actions. This integrated concept fits well with the Grant (1996) concept that production requires the coordinated efforts of many specialists, including internal auditors and risk managers.

As was outlined in the literature review, Winter (1986) suggested that KM is evidenced by routines, or designed patterns that assist in the transfer of knowledge. The company risk assessment process, resulting in the risk register, is a good example of such a routine. Usually underpinned by COSO or ISO 31000, both the auditors and the risk managers need to understand the routines involved in assessing risks. Indeed, the more that this assessment process is common to both the auditors and risk managers, the greater the competitive advantage.
Secondly, Galbraith (1973) outlines that group problem solving and decision making is a key feature of transferring tacit knowledge to explicit knowledge. A combined board audit and risk committee is an example of such a process.

The risk managers present a risk assessment and risk register to that committee. The auditors test that assessment, which requires many of the tacit skills used by risk managers, and identify gaps that translate into new risks. The outcome is then discussed at board committee level with both the internal auditors and risk managers present. The group decides which risks are highlighted, what mitigations are pursued and what new risks should be added to the register. The management program for mitigation is also agreed at this committee, which serves to translate the experienced tacit knowledge of board members, risk managers and auditors, into explicit actions for managers and other employees.

Nonaka and Takeuchi (1995) noted that another feature of KM is a common body of knowledge shared by different disciplines. That body of knowledge includes language, symbolic communication and recognition of one another’s individual knowledge domains. Both internal auditors and risk managers use the shared definitions found in the ISO 31000 terminology. The concepts of risk likelihood, risk consequence, residual risk, the risk register and internal controls are fundamental to both internal audit and risk management. The symbols of statistical method, sampling, probability distribution and confidence levels form a common language for both disciplines (Moeller, 2004). The auditors, the risk managers and the board committee members understand the knowledge domains of each discipline. That means they can work together, combining and building on the team members’ abilities, using a commonly understood language.

It seems that the integration of internal audit and risk management, both at the functional and board committee level, shows some strong elements of knowledge management.
4.4.2 Three Lines of Defence

According to the survey responses, the synergy between audit and risk is driving the formation of combined board audit and risk committees. An alternate, but linked definition of synergy, as portrayed by the respondents to interviews is the “three lines of defence” model. This model is discussed in Chapter Two and is heavily utilised by financial institutions (Micallef, 2008).

The three lines of defence model adopts three barriers in the management of risk:

1. The first barrier is having solid management. Good managers comply with policy and process, scan for risk and implement sound internal controls;

2. The second barrier is the risk assessment and management process. This process leads to a focus on risk and implementation of sound mitigations; and

3. The final barrier is both the internal and external auditors. These functions are looking to assure the board on the adequacy of internal and accounting controls and the effectiveness of risk management.

A finance company executive summarised this model:

We use the three lines of defence model, the first line being management, the second being risk management and the third is the internal and external auditors. (CFO from a GICS 40 company.

While this model requires no integration between internal audit and risk management, both interview and survey respondents raised this model as a form of synergy between management, audit and risk. The argument put forward was that audit and risk are two of the three components to the above system, and hence a synergy within that overall system.
Respondents suggested that the adoption of the three lines of defence model would be better facilitated by a combined board audit and risk model. Such a model allows one authority to preside over both the identification of risks and the controls for such risks. Having conversations between the three components (management, the risk managers and the auditors) in the same forum was cited as a much more efficient use of resources for the three lines of defence model. This aligns with the KM approach noted above as discussions in the same forum help transfer tacit to explicit knowledge.

In the above context, this type of synergy works within the concept of independence as raised in Chapter Two. Internal audit and risk management can be kept separated at the functional level, but combined as pieces of overlapping governance at the board committee level. This situation was confirmed by two executives, both from the financial services sector:

*Under the three lines of defence model, risk and audit must be kept separated to ensure that the three lines do not merge into two or even one line of defence.*  
(CRO from a GICS 40 company)

*Internal audit is intentionally kept independent from risk management and from general management.*  
(CAE from a GICS 40 company)

One respondent, a risk management partner in a Big Four practice, saw a problem with the current structure of the three lines of defence model:

*There is some talk of three lines of defence, with internal audit being the third line of defence. I dislike this taxonomy as it attempts to suggest that having a strong, vibrant and skilled internal audit function is relegated to the third line of defence, when I would argue it could act as a first line of defence against complacency and setting the right high performance tone of a business.*  
(Risk Management Partner - Big Four)
There is no suggestion in the three lines of defence model that internal audit is any less important than robust management or sound risk management.

Throughout this research the three lines of defence model has been raised, mainly by GICS 40 financial services companies. This industry specific aspect may be underpinned by contingency theory where environmental factors facing banks suit such a model. In Chapter Two, the Walker Report (2009) saw financial institutions as having a core business of risk management. Perhaps this unique environmental factor, the core business risk aspect of banking, is driving the need for multiple lines of defence.

4.4.3 Accounts are the Culmination of Risk Management

Another view expressed, by interviewees, on the synergies between internal audit and risk management was not anticipated by the author. Several of the interviewees raised a different synergy, related to approving the annual financial statements. One executive, in the comments to the survey, wrote:

> The ultimate aim of the audit committee is to deal with the financial statements. These statements are derived from the performance of the company, which is the culmination of taking opportunities and managing risk. (COSEC from a GICS 15 company)

The following figure, which was suggested by an interviewee, sheds light on this view and provides further support for the integration of the internal audit and risk management functions at a number of different levels:
As explained by an interviewee using the above figure, the annual accounts are the “tip of an iceberg”, or the culmination of the years’ activities. The accounts are derived from strategy formulation, work to enhance opportunity and minimise risk through the application of internal controls and thorough risk management. Broadly, the annual financial accounts are the “report card” indicating how well the risks have been managed and how well opportunities have been leveraged during past trading periods.

This view is effectively saying that all ongoing normal operations are, in reality, an exercise in risk management. This fits with the McNamee and Selim (1998) philosophy discussed in Chapter Two:

*Productive organisations seek to utilise their assets to create value. This requires interaction between the internal and external environment, which creates risk. The management of this risk keeps the organisation viable and productive.*

*(McNamee and Selim, 1998)*
A consumer discretionary company executive commented:

*Audit is all about the annual accounts and the balance sheet but these are just the outcome of all underlying opportunities, threats and how risks are dealt with. The accounts are just the “tip of the iceberg”. (CRO from a GICS 25 company)*

It would seem incongruous to have the risks assessed and mitigated through one committee and the annual accounts reviewed and endorsed through another, when the accounts, according to interview respondents, are a direct outcome of the management of risk. In the words of a materials company executive:

*Having risk management in the audit committee gives the audit committee a more holistic view of the business operations, the wins and losses, and ultimately helps with the integrity of the accounts. We have an annual risk workshop facilitated by KPMG under the auspices of the audit committee. The risks developed are reviewed throughout the year via management presentations to the audit committee. (COSEC from a GICS 15 company)*

Another executive from a financial services company agreed:

*All the risks, occupational health and safety (OH&S), health safety and environment (HS&E), construction, finance and debt, are pulled together and overseen by the board audit committee. The culmination of managing all those risks is the financial report, which in many ways, is the output of the audit committee. (CRO from a GICS 40 company)*

The audit committee is one of the most important agency costs. The audit committee sits above management, consists of independent directors and in many respects controls the agent’s behaviour. A combined audit and risk committee is heavily involved in the oversight of risks which arise from day to day activity. When this oversight of risks and knowledge of the business is combined with authority for the annual accounts, a potent mix is created.
Surely from an agency perspective having the keeper of the accounts also overseeing risk management, or the events that can impact on the accounts, must result in a better outcome for the principal.

Having the financial accounts dealt with by one board committee, and the driver of the annual accounts, risk management, dealt with by another committee seems sub-optimal. Separate board risk management committees would add a layer of agency costs to the governance framework and make the links between risk management and internal control more difficult to co-ordinate.

An industrial company executive added:

*Traditionally the audit committee dealt with financial risk which brings in a risk perspective. Managing risk is integral to presiding over the integrity of the annual accounts in that internal controls and processes must be working properly.*

*(CRO from a GICS 20 company)*

The concept of synergy being derived from the relationship between risk management and the annual accounts may also bring a KM flavour to that synergy. If it is agreed that the annual accounts are the result of, or a report card on, risk management activities then KM may play a role. The combined board audit and risk committee is one of the only places inside the company where the risk assessments, risk plans and mitigations and resulting financial reporting intersect and can be monitored and measured.

The audit committee is probably the only forum where independent director experience, audit testing, risk assessment and financial outcomes are reviewed as a complete package. In that committee, all the elements required for KM are present. A common language both over risk management and the annual accounts is present.
The players all understand the tacit world of risk methodology, the IIA procedure and the International Accounting Standards (IAS). The symbolic communication provided by ISO 31000 and IAS statements is utilised and understood.

All the players have intersecting knowledge, but not the same knowledge. The board members emphasise alignment with IAS while understanding the risk implications. The risk managers can compute the risk outcomes while still broadly understanding the IAS drivers. The auditors understand both ISO 31000 and IAS concepts, but bring a strong internal control emphasis to areas that may not be performing in a financial sense.

The combined board audit and risk committee is really a production environment set up to coordinate the efforts of many specialists who each contribute different knowledge, each facet building on one another. That tacit, skill based knowledge is then converted by that committee into explicit plans and actions that the remainder of the company can grasp and carry out as daily activities.

### 4.4.4 Similarity between Internal Audit and Risk Management

A number of interviewees pointed out that the similarities between internal audit and risk management add to the concept of synergy and promote integration between audit and risk. The overlaps between internal audit and risk management were also discussed in Chapter Two, section 2.11.

Audit and risk are both governance functions. Regardless of the board committee arrangement, both internal audit and risk management are agency controls put in place by boards to provide assurance over the activities of the company. In the words of an industrial company interviewee, this agency perspective of the principal controlling the agent is seen as:
Both risk management and internal audit are systems put in place by boards to monitor the health of the organisation. They both report on the success of management actions in pursuing the organisation's objectives. (CRO from a GICS 20 company)

Both audit and risk operate in a similar manner. The centralised risk management function assists management with their responsibility to identify, monitor and mitigate risk. Likewise, the internal audit function assists management with their responsibility to incorporate sufficient internal control to safeguard the assets of the business. One executive from an industrial company, when interviewed stated:

Both functions (audit and risk) are “all care, no responsibility” functions where management is responsible and both audit and risk provide a consulting, facilitation and system administration role. (COSEC from a GICS 20 company)

A telecommunications company executive linked risk management to internal audit:

Internal audit is all about internal controls. Internal controls are put in place to manage risk. The Board are interested in financial reporting controls which again are directed at managing risk. Also the ASX principles link audit and risk. (CRO from a GICS 50 company)

Grant (1996) outlines the importance of commonality and common knowledge domains as being fundamental to knowledge management. Commonality in specialised knowledge underpins the sophistication of knowledge integration. If both the auditors and risk managers understand that they are facilitators to management, without having direct responsibility for controls, then they share a common understanding of tools and techniques for that facilitation role. This helps transfer tacit understanding into explicit knowledge and actions. The shared understanding of this facilitation role means that auditors and risk managers can work together to integrate and transfer knowledge.
The compliance function was also drawn into the synergies between audit and risk by several respondents from Managed Investment Schemes.

### 4.4.5 Alignment with Compliance

During the interviews with the financial services executives, the role of compliance was added into the explanation of audit and risk synergy. Like risk and audit, the compliance role is one of facilitating a management responsibility to comply with legislation and policy. The compliance manager plays a similar role to the risk manager, providing policy, procedure, a compliance system and reporting for management. One interviewee from a financial services company stated:

> If we have a compliance breach, a breakdown in controls, then internal audit dive in to ascertain the cause and effect and then suggest controls that may solve the problem. (CFO from a GICS 40 company)

In summary, synergy was defined by respondents in three components. Firstly, the “circular flow” between audit and risk where the auditors use the risk process to design their program then find new risks to feed back into that risk process. Secondly, risk management forms one barrier of the “three lines of defence” system which is gaining popularity. Finally, the fact that the annual accounts are in reality, the summation of how risks have been managed was seen as an added synergy between audit and risk at the board committee level.

Understanding these synergies helps resolve research objective one and two. Both the structure of risk management in leading Australian companies and integration between internal audit and risk management rely on this synergy as a strong driver for change.
The research showed that 73% of S&P/ASX 200 companies are governing risk management through the board audit committee. This confirms prior research completed by KPMG (2005) and Subramaniam et al (2009). The reason for this is the natural synergy between internal audit and risk management.

To the author’s knowledge, this study has been the first to identify the reasons behind combining board audit and risk committees. The concept of synergy may also be underpinning the current trend towards the integration of internal audit and risk management.

The above finding satisfies part of the first research objective. That objective sought to establish the number of S&P/ASX 200 companies that govern risk management through the board audit committee, and why that approach is preferred.

The synergy between internal audit and risk management presents a strong argument for a combined board audit and risk committee. Given that outcome, why do 17% of S&P/ASX 200 companies have a separate board risk committee?

4.5 SEPARATE BOARD RISK COMMITTEES

This section looks at the 17% of S&P/ASX 200 companies that have a separate board risk committee. These companies have both a board risk committee and a board audit committee to provide agency control.

Contingency theory would suggest that some Australian companies will adopt alternatives to the board audit committee to govern risk management. In other words, environmental factors, such as size, industry grouping or regulatory scrutiny may impact on the decision to combine or separate the board risk committee from the board audit committee.

Looking back at Figure 4.1, the desk-top analysis indicated 17% of S&P/ASX 200, companies, had a separate board risk committee.
The following Figure 4.7, which is taken from the desk-top analysis, shows the breakdown between combined board audit and risk committees and separate board risk committees for the Global Industry Classification Standard GICS).

**Figure 4.7  Separate board risk committees by GICS**

There are three prominent features to this graph:

1. the high proportion of separate board risk committees in the financial services sector (GICS 40);

2. a similarly high proportion of separate board risk committees in the consumer discretionary and consumer staples sectors (GICS 25 and 30); and

3. the lack of a separated board risk committee in the GICS categories, 45, 50 and 55 (Information Technology, Telecommunication and Utilities).

The most prominent feature of Figure 4.7 is the high percentage of separate board risk committees in the GICS 40 category of financial services. While overall, 17% of S&P/ASX 200 companies have a separate board risk committee, in GICS 40, 32% percent of companies have a separated committee.
4.5.1 The Financial Services Sector (GICS 40)

Thirty two percent of financial services companies have set up a separate board risk committee. This is nearly double the 17% of the overall S&P ASX 200 companies that have a separate board risk committee. The survey questions sought answers for this high concentration.

The results for question six of the survey, as to why a separate board risk committee was chosen, were graphed. Six alternative factors were established during pilot interviews. The respondents were asked to score each factor from one to five, one being of no importance and five being very important. The factors are outlined in Appendix Three and are listed below.

The following graph, Figure 4.8 summarises the responses for survey respondents who were in the GICS 40 sector and had a separate board risk committee. The graph highlights the reasons for having a separate board risk committee.

![Figure 4.8 Reasons for separate board committees in GICS 40 financial services companies](image-url)
An average score of two point five indicates the point of indifference, scores above two point five indicate that the rationale becomes more important and scores below two point five indicate lesser importance. It appears that all six factors contribute to the adoption of a separate board risk committee. These factors are, from left to right:

1. to manage specific financial risks;
2. to assist with the implementation of ERM;
3. the regulator requires evidence of strong risk management;
4. a separate board risk committee is industry standard;
5. the risk committee has evolved from former credit committees; and
6. to signal that we focus on risk management in the high profile area in which we operate.

The highest response, scoring 4.5, was to signal a focus on risk management in the high profile area in which we operate. As noted by Morris (1987) and Certo (2003), signalling theory is based on information asymmetry in markets. That theory suggests that firms will benefit from the disclosure of new or improved governance initiatives that create a favourable impression in the market. The financial sector sees a benefit in conveying to the market that they have a separate board committee dedicated to risk management.

That signalling theory aspect also picks up the requirement by regulators, as outlined in Chapter Two, to show a strong risk management presence. As an example, two GICS 40 interview respondents in the financial sector stated:

The board felt that setting up separate Risk and Compliance Committees at board level sent the right message to the regulators that we focus on risk. (CFO from a GICS 40 company).
Really set up under AFMA, ASIC and Basel. Basel defines nine operational risks that need to be monitored in a banking environment. (COSEC from a GICS 40 company).

This signalling theory aspect is supported by the Liebenberg and Hoyt study in 2003. They found that the financial health of companies in the finance and energy industries is opaque to investors due to the lack of tangible assets.

Therefore, the arrangement of a separate board risk committee may reduce information asymmetry and signal to outside stakeholders that risks are well controlled.

The next highest rated response, a score of 4.4, was for the management of financial risk. This aligns with the contingency theme in the literature that the core business of banks is the management of risk (Walker Report, 2009). In Chapter Two, Goodwin-Stewart and Kent (2006) and Carcello (2005) suggested that finance companies are more risky, are highly regulated and face more compliance risks than other companies. Working in an environment rich in financial risk may be prompting the development of separate board risk committees. The interviews with CROs from the banks and property trusts supported Figure 4.8. Companies that traded in risky derivates, such as interest rate, foreign exchange or energy related swaps, tended to use separate board risk management committees. Failure to appropriately manage derivate trading can lead to massive losses as has been seen in a number of corporate collapses including Bearings Bank Ltd and more recently Societe Generale S.A. in Paris.

One high profile executive from a major Australian bank commented:
A separate board risk committee is industry standard for the banking sector because of the specific types of risk and the huge consequences of poor risk management. These committees look at the following risks: credit, market, trading, operational, security, liquidity, capital, compliance and regulatory. Compliance and regulatory risk obligations are very tough in the banking sector, with a high level of regulatory scrutiny. (CRO from a GICS 40 company)

This comment contains aspects of institutional theory, contingency theory and signalling theory. Industry standard means that companies gravitate towards the practice, an institutional theory outcome.

Managing specific types of risk goes towards a contingency approach where the environment is driving the response. Regulator scrutiny would see signalling theory as a driver for the committee arrangements.

The evolution of board risk management committees from former management committees within the banking environment is perhaps another example of a contingency theme. Lawrence and Lorsch (1967) contend that the governance structure depends on environmental factors. Structures will evolve over time as the environment changes. Organisations that can best adapt to the changing environment will survive. The contingency theme came across strongly in the interviews. Two bank executives explained that situation:

The bank has a separate risk and compliance committee which arose from a former credit committee which had a lending authority. The committee looks after credit and operational risk, asset and liability [liquidity] risk, but not ERM across the business. (CRO from a GICS 40 company)
The board risk committee evolved from a credit committee and a finance committee. The committee deals with investment risks in approving investment mandates. (CRO from a GICS 40 company)

The above comments raise an agency theory issue of management involvement in the board committee. If separate board risk committees evolved from former management committees, are these committees acting as proper board committees, protecting the principal, or are they dominated by management, the agent? In other words, are the longer term views of the principal or the shorter term views of the agent being represented on such committees? Answering that question would require specific focus on the banking sector and is research for another day.

The fact that some of these separate board risk committees, in the financial services sector, have been split off from former audit committees may also be significant. Two financial services executives made the following comments:

*Set up to provide a separate focus to the audit committee. The risk committee holds a lending authority which is not appropriate to an audit committee.* (CAE from a GICS 40 company)

*Stems from prior audit and risk committee, where workload was too big and committee was split into two. That allowed the financially literate directors to concentrate on the annual accounts and the more generalist directors to focus on business risks.* (CFO from a GICS 40 company)

The issue of committee workload is dealt with later in this chapter.

A number of respondents raised the problem of “turf wars” between separate board audit and board risk committees. The problems associated with having risk management considered by one board committee and audit matters by another, reinforces the concept of synergy with respect to an integrated board committee.
The argument raised was that, given the strong synergies between audit and risk, separating the audit and risk committees, at board level, will lead to demarcation disputes over the work of each committee. In other words, the line at where audit committee work stops and risk committee work commences becomes blurred. The respondents cited issues such as:

1. the audit committee not being informed about serious risk issues that are being investigated; and
2. the risk committee not readily accepting audit committee suggestions for the improvement of risk mitigations.

These turf war issues or a non-alignment between board audit and risk committees go against the concept of knowledge management. KM indicates that board committees should work together to convert complex knowledge into information that can be shared by the organisation.

A materials company executive advised:

_In regard to synergies, I see the flip side as more important. Because risk and audit are so closely aligned and overlap, having separate board committees would cause unnecessary complications. The board committees would be continually competing over jurisdiction and what falls into what committees' area of expertise._ (COSEC from a GICS 15 company)

An alternate explanation for these turf conflicts may come from power theory. Each committee, the board audit and the board risk committee consists of powerful players seeking to exert their influence over the direction of the company. Dominant groups use coercion, influence, authority, force and manipulation to secure their objectives. The synergies between audit and risk mean that both committees overlap and the more powerful directors may become competitive. In such a case the power objectives of individuals displace the harmonies from KM.
Finally, the propensity to set up separate board risk committees in the finance sector could be an example of DiMaggio and Powell’s (1983) mimetic isomorphism. The uncertainty in the financial sector, given the risky nature of derivative trading may be a powerful force encouraging imitation with peers.

There appears to be very little prior research on why the financial sector is choosing separate board risk committees. Both signalling and contingency theory aspects provide an explanation. Financial institutions are trying to reduce information asymmetry by signalling to markets that the separate board risk committee has a focus on risks.

The specific environment facing the banking industry, where managing financial risk is a core business activity, might also be driving the adoption of separate risk management committees. However, this finding needs to be treated with care, as 55% of GICS 40, financial services companies still have a combined board audit and risk committee.

The next significant finding is from the GICS categories 25 and 30, or consumer discretionary and consumer staples. In these combined categories approximately 26% of companies have a separate board risk committee.

The following section uses the information gained from the surveys and interviews to help explain why a higher proportion of consumer products companies have developed separate board risk committees.

4.5.2 The Consumer Products Sector (GICS 25 & 30)

From the desk-top analysis data-set (see Appendix Two) there are thirty five companies out of two hundred in the GICS 25 and GICS 30 sectors. Of these thirty five companies, nine companies or 26% have a separate board risk committee.
Survey question six (Appendix Three) asked respondents with separate board risk committees why such a model was chosen. The question gave respondents six possible reasons and asked them to rank each on a five point Likert scale.

Figure 4.9 graphs the responses from the survey respondents in the GICS 25 and 30 sectors who indicated that they had a separate board risk committee.

![Figure 4.9 Reasons for adopting a separate board risk committee in GICS 25 & 30 sectors](image)

An average score of two point five indicates the point of indifference, scores above two point five indicate that the rationale becomes more important and scores below two point five indicate lesser importance. Three reasons are more significant:

1. to manage specific financial risks;
2. to assist with ERM; and
3. to signal that we focus on risk management in the high profile area in which we operate.

Six of these companies were interviewed and the impact of signalling theory came across more strongly in the interviews than was indicated in the survey responses.
Three of those interviewed stated that having a separate risk committee was underpinned by the need to focus on, and signal a focus on, industry specific risks. This supports the signalling theory approach, as outlined by Morris (1987) and Certo (2003), and discussed in Chapter Two. One of the interviewees was in the food processing industry:

*Our risk committee is driven by the board demanding a focus on the specific risk of food hygiene. We used to have a combined committee, but the board risk committee is now separate.* (CRO from a GICS 30 company)

A consumer discretionary company executive reported a similar theme:

*This company is high profile and the operational risks are very specialised. A separate risk and compliance committee was established to focus on those risks in a forum removed from financial and prudential matters.* (COSEC from a GICS 25 company)

Providing further support for the signalling theory theme, one interviewee stated that, with the advent of the new ASX Principle Seven, which requires a much higher focus on risk management, a separate risk committee was created.

*To place a higher focus and emphasis on risk management.* (CRO from a GICS 30 company)

Having a separate board risk committee to oversee the implementation of ERM emerged as a strong theme from both the survey and interviews. A consumer staples group executive talked about the implementation of ERM:

*The audit committee looks after financial risks while the risk committee looks after operational risks.* (COSEC from a GICS 30 company)
In a similar manner, an executive from a consumer discretionary company noted:

*The risk committee deals with operational risks, including OH&S and business continuity. The audit committee just concentrates on the financials.*  (CRO from a GICS 25 company).

This ERM implementation theme continued with a consumer discretionary retailer:

*The main driver for the creation of a separate risk management committee is the developing culture of risk management across the company. It is now recognised as a major governance requirement that needs to be subject to far greater scrutiny than was happening in the audit committee. A focussed committee for risk management is seen as a step up the maturity ladder.*  (COSEC from a GICS 25 retail company).

Finally, committee workload was also cited as a factor. Three of the interviewees stated that having a single committee was driven by committee workload issues, that is, there is too much work for one combined board committee. One executive from a consumer staples company reported:

*The risk committee and the audit committee are basically the same people, but in separate committees they dedicate time to look at each area, financial controls and risk, away from the other.*  (COSEC from a GICS 30 company)

The committee workload issue is further discussed in section 4.7 below.

### 4.5.3 Three Sectors without Board Risk Committees

Figure 4.7 indicated that industry sectors GICS 45, 50 and 55 do not appear to have any companies with a separate board risk committee.
From the desk-top analysis GICS 45, information technology, contains three companies, all of whom have combined board audit and risk management committees. The average revenue for these three companies is $980 million, which is far below the overall average for the S&P/ASX 200 of $3,443 million.

This could indicate that these GICS 45 companies might be too small or have an insufficient number of directors to have multiple board committees. Subramaniam et al (2009) found that the existence of risk committees increased with organisational size.

GICS 55, utilities, contains twelve companies, eleven of which have a combined board audit and risk committee and one of which has no board risk committee. The average revenue for these twelve companies is $823 million, which again is far below the overall average for the S&P/ASX 200 of $3,443 million. This again indicates that these GICS 55 companies may be too small to split board committees into both risk and audit.

Finally, GICS 50, telecommunications contains three companies, all of which have combined board audit and risk committees. Since these three companies include two large national carriers, the average revenue of $13,304 million is far above the S&P/ASX 200 average of $3,443 million. However, this sample may be too small to draw any definitive conclusions. It does seem however, that company size might feature in the decision to maintain a combined board audit and risk committee in these GICS sectors. Company size was noted by Subramaniam et al (2009), Ruigrok et al (2006) and Benz and Frey (2007) as an agency cost related factor. The general thrust of these works was that larger companies had better resources to set up multiple board monitoring committees. In smaller companies, the expense of maintaining agency control through a separate board risk committee may not be justified, i.e. they cannot afford it.
Moving back to the entire population of companies with separate board risk committees, an interesting finding was that GICS 35, the health care category, had a very low proportion of companies with a separate risk committee. Intuitively, one would expect that companies dealing with the manufacture of health care products such as blood products, vaccines or medical equipment, might set up a separate board risk committee to reinforce the focus on risk and signal such care to the investment community.

However, that appears not to be the case. Perhaps, as suggested by Brown, Steen and Foreman (2009) these high technology companies are delegating risk management to dedicated ethics and patient safety committees.

Finally, the full population of S&P/ASX 200 companies have on average revenues of $3,443 million. The 17% of the population which have separated the board audit and risk committee had, on average, revenues of $4,211 million. This indicates that companies that have separate board risk committees tend to be larger companies. This aligns with the Subramaniam et al (2009), Bradbury (1990) and Piot (2004) agency theory based findings that board risk committees are set up by companies with larger boards. However, since most of the large banks are included in this sample, and the banks have revenues far above the average, this sample is skewed upwards. It is difficult to determine whether size or industry classification is a primary driver and thus whether contingency theory or mimetic isomorphism explains these results.

An outcome from the above analysis into board committee structure is that risk management in the S&P/ASX 200 is primarily governed through the audit committee at board committee level. Given that the Canadians are leaders in adopting ERM, with Colquitt et al writing about risk management structures as early as 1999, this finding may be driven by mimetic isomorphism. Australian leading companies appear to be adopting a similar approach to that utilised overseas.
The prevalence of board audit committee oversight of risk management also shows that a strong level of integration is occurring between internal audit and risk management at the board committee level.

From an agency perspective, having the audit committee overseeing both the risk management involved in daily activities, and the annual accounts which result from those activities was suggested by those interviewed to be a good practice.

Having the same committee reviewing both the internal controls and risk responses may be a lower cost and a more effective level of governance.

Apart from Subramaniam et al (2009), there is very little previous literature on separate board risk committees. Therefore, one of the research objectives for this study was to establish whether S&P/ASX 200 companies are setting up separate board risk committees. Seventeen percent of Australian companies have a separate board risk committee. This separate risk committee was more prominent in the financial services and consumer discretionary sectors. The main driver for the separate committee was explained by signalling theory. Banks want to reduce information asymmetry by highlighting their risk management governance. Consumer products companies want to show that risk management is important in the high profile areas in which they operate. Contingent environmental factors, specific to the financial sector may also be driving the higher proportion of separate risk committees. The financial services sector has the board risk committee concentrate on credit, market, trading, operational, security, liquidity, capital, compliance, regulatory and lending mandate risks.

Using a separate board risk committee to assist with the adoption of ERM was identified by some companies in the GICS 40 category and in the GICS 25 and 30 sectors.
However, using the committee to signal a commitment to risk management and to manage financial risk was seen as more important. The facilitation of ERM may be of a second order.

The desk-top analysis revealed that 55% of the banks use the board audit committee to oversee risk. Indeed, interviews revealed that the separate board risk committee has problems such as demarcation disputes with the audit committee members. Originating from former credit and lending mandate committees, those committees may be heavily influenced by management.

Separate board risk committees tend to focus on market and trading risks rather than holistic risk management. Separate board risk committees cannot capitalise on the synergy between audit and risk and demarcation disputes may arise over committee boundaries with the board audit committee.

4.6 NO BOARD RISK COMMITTEE

Turning to the final 10%, made up of twenty S&P/ASX 200 companies in Figure 4.1 that have no observed board risk management committee. For clarity, these companies state in their annual reports that risk management is handled by the full board, a management committee or by management.

The first thing to note is that these companies are small. The average revenue for these companies is $869 million compared to average revenues of $3,443 million for the full population of S&P/ASX 200 companies. Therefore the agency cost related factor of company size, as outlined by Subramaniam et al (2009) may be driving this outcome. These companies may be too small to bear the agency costs of having a board risk management committee.

Twenty five percent of companies with no board risk management committees are in the CIGS 15 materials category, most of which are small mining companies. Life-cycle theory would see these companies as being in the birth or early growth stage.
At this stage, revenues are small, cost control is paramount and the structures are simple. The more mature forms of agency control such as board committees may be many years away. These companies are still in the development stage, where revenues are small and risk management may not yet have reached maturity. Indeed one of these companies had yet to earn any revenue at the time of the study.

The comments provided in the survey responses shed some light on this issue:

Our company is a young company and the board are just getting on top of risk management. The risk management function is evolving, soon to be formally implemented. (CFO from a GICS 15 company)

Enterprise wide risk management is only now just being embraced by the company. We previously focussed on financial risk. (CRO from a GICS 25 company)

We are half way through a three year implementation plan. (CFO from a GICS 25 company)

Thirty five percent of the companies with no board risk management committee are property trusts, and in each case, the trusts are part of a larger banking or insurance group. While still publicly owned and listed, these trusts may rely on the risk management expertise of the parent bank or insurance company rather than developing their own board committee.

In the desk-top analysis the corporate governance statements and annual reports for all twenty of these companies with no board risk committee were studied. Eleven of the companies stated that they had risk committees at the executive level to deal with risk management. The other nine stated that the full board provided oversight of risk management:
The chairman is not keen on merging audit and risk as he wants the full board present when significant risk issues are being discussed. (CAE from a GICS 10 company)

Companies with no board risk committee have not been discussed in previous literature. It appears that these companies tend to be small companies such as mining start-up companies. These companies may not be able to afford the agency costs of having a board risk management committee. Where no board risk committee is present either the full board or an executive committee takes on the risk management role.

We now turn to the problems that companies with combined board audit and risk committees are experiencing finding sufficient skilled directors and sufficient time at meetings to deal with the workload arising from both audit and risk matters.

4.7 SKILL, WORKLOAD AND TIMING ISSUES

Approximately 70% of the S&P/ASX 200 companies govern risk management through the board audit committee. One of the research objectives of this study was to establish whether this combining of risk, audit and financial reporting is causing any skill, timing or workload issues at board committee level.

Chapter Two outlines the problems that some international companies are having with integrated board audit and risk committees. These issues are discussed by Spira and Page (2002), Zaman (2001) and Fraser and Henry (2007). In essence it is argued that combining the board audit and risk committees produces too heavy a workload for directors. Firstly, there will not be sufficient time at board audit committee meetings to cover the agenda for both audit and risk matters (Alles et al, 2005). Secondly, finding directors with skills in both financial matters and risk management may also be difficult (Cohen et al, 2002 and Blue Ribbon Committee, 1999).
In contrast to the issues outlined above, this research found that generally, skill, timing and workload issues were not significant problems in the leading S&P/ASX 200 companies. Question five in the survey (see Appendix Three) was directed to companies with combined board audit and risk committees. The question asked about the relevance of four factors in regard to this issue:

1. difficulty in finding directors with both risk management and financial skills;
2. difficulty finding directors with risk management skills;
3. difficulty finding directors with financial skills; and
4. difficulty finding enough time at board audit committees.

Figure 4.10 below outlines the responses. The respondents were asked to rank each issue on a five point Likert scale ranging from no problems at one end to significant problems at the other end.

As can be seen from the chart, the average response from all survey respondents was less than two point five, therefore tending towards the “no problems” end of the scale. This was confirmed by several comments provided in the surveys. One telecommunications company executive wrote that:
The financial competence of directors is not an issue. We recently appointed an ex-KPMG partner who is very experienced in ERM. (Survey comment provided by GICS 50 company)

A GICS 40 financial services executive noted:

Directors with financial skills automatically have risk skills. (Executive from a GICS 40 company)

A GICS 20 industrial company executive commented that:

The key issue is the frequency of meetings. (CFO from a GICS 20 company)

Although on average, the S&P/ASX 200 respondents reported no issues with skill, workload or timing, some companies did report problems. Sixty eight companies responded to the survey that they had a combined board audit and risk committee.

Of these 68 companies, 17 respondents, or 25% reported some issues with workload and timing. The seventeen respondents scored between four and five on the Likert scale, indicating that they had an issue with committee workload. These issues appear to be related to the increased workload of board committees brought on by risk management as identified by Harrison (1987) and Alles et al (2005) in Chapter Two.

Four companies that indicated they had skill, workload or timing issues were able to be interviewed. When asked how they were dealing with these issues they tended to spend the majority of the audit committee meeting on one issue, audit or risk, depending on the time of the year. For 30 June year end companies, it was typical for meetings around strategy time, October to March, to deal with risk issues. Meetings held in the period over year end, April to August, dealt with annual account matters.

One interviewee reported:
The board audit and risk committee currently meets five times per annum for three hour sessions. Two are about annual accounts and three meetings have a risk flavour. We are currently reviewing our charter to determine whether we add another meeting or move to four hour meetings. (CFO from a GICS 10 company)

Another stated:

The meetings around financial year end are predominantly about finance and accounting matters. The meeting around strategy time is largely about risk. (COSEC from a GICS 20 company)

A telecommunications company executive stated:

Our risk management is governed by the audit committee, which is a sub-committee of non-executive board members. Two of the six audit meetings have a specific risk agenda item included in the meeting. Management make presentations to the audit committee on their implementation of controls to mitigate risk. The amount of time explicitly focusing on risk issues at audit committee is considerably less than financial issues, but if there are risk issues that need attention then time is made in the agenda. (CRO from a GICS 50 company)

Finally, an executive from an engineering consultancy added:

Originally the audit and risk committee met only twice per annum. Now that we are taking a stronger focus on risk, and with the addition of an internal audit function, we are increasing the frequency to four or even six meetings per annum. (CAE from a GICS 10 company)

The comments provided in responses to question five of the survey supported the same theme. Two executives, one from a consumer staples company and one from an industrial company commented that:
We introduced more audit, risk management and compliance committee meetings and lengthened their duration. (COSEC from a GICS 30 company)

The chair of the audit and risk committee was a partner at PWC, which brings both financial and risk management skills and experience. The proportion of meetings devoted to financial versus risk management varies throughout the year. Generally a suitable balance is maintained. Increased focus on financial matters at year end is often managed through a longer time allocation for overall meetings, or structuring meetings over two sessions. (COSEC from a GICS 20 company)

This splitting of the audit committee into two components; (a) a time to consider risk; and (b) a time to consider financial matters; raises some philosophical questions. How different is the combined audit and risk committee model to having a separate board risk committee? If the combined audit and risk committee meets separately on audit and separately on risk, and has the same members, are there in fact two committees? One consumer discretionary executive commented:

The risk committee and audit committee are basically the same people, but they dedicate time to look at each area (risk and audit) away from the other. (CRO from a GICS 25 company)

Another interesting finding was that nine out of the sixty eight survey respondents, who had a combined board audit and risk committee, indicated they were experiencing difficulty with finding directors who have strong risk management skills. One interviewee, from the financial services sector, stated:

Our directors receive around $30K per annum in remuneration. The risk management skills that we require have a market value of between $200K and $500K per annum. Potential directors are either working in high reward occupations or have taken early retirement. (CRO from a GICS 40 company)
While this issue only affects a small number of respondents it partially supports the Zaman (2001) and Spira and Page (2002) contention that combined board audit and risk management committees may be light on risk management skills. Whether this is impacting on the committee’s ability to function, as portrayed by Harrison (1987) and Alles et al (2005) is difficult to gauge given the small number of companies experiencing such problems.

Generally leading Australian companies are not experiencing the problems noted by Spira and Page (2002), Zaman (2001) and Fraser and Henry (2007) with finding appropriately qualified directors and sufficient time at meetings.

It appears that combined board audit and risk committees focus on audit matters around year end (April to August) and risk matters during the strategy/planning period (October to May).

This finding satisfies another part of the first research objective. That objective included the need to establish whether leading Australian companies are experiencing skill, timing or work-load problems with the addition of risk management to the board audit committee.

4.8 ENTERPRISE RISK MANAGEMENT (ERM)

Before moving on to the executive management level of governance, the findings on the development of ERM in leading Australian companies are worth noting. This section addresses the extent to which ERM has been adopted in the S&P/ASX 200 companies. The development or maturity of ERM implementation has been studied overseas by Beasley et al (2005), Gramling and Myers (2006) and Miccolis et al (2001). To date there has been no previous work on this issue in Australia.

Question two of the survey (see Appendix Three) asked respondents to rank the extent to which they had adopted ERM in their organisation.
The ranking instrument was a five point Likert scale, ranging from one being rejection or unawareness of ERM through to five being a fully mature ERM system. The scales were based on previous work by Beasley et al (2005) and Gramling and Myers (2006) as discussed in Chapter Two. Those previous works were used to assign an ERM development metric to each grading, as follows:

<table>
<thead>
<tr>
<th>Likert Scale</th>
<th>State of ERM Development</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ERM unaware</td>
</tr>
<tr>
<td>2</td>
<td>ERM under investigation</td>
</tr>
<tr>
<td>3</td>
<td>ERM partial framework</td>
</tr>
<tr>
<td>4</td>
<td>ERM in place</td>
</tr>
<tr>
<td>5</td>
<td>ERM fully mature</td>
</tr>
</tbody>
</table>

*Figure 4.11 State of ERM development in S&P/ASX 200 companies*

This ranking metric is really a self assessment however it may the only way to measure ERM implementation absent a standard on company maturity. This assessment does however allow the overseas work to be compared to the Australian results.

The ERM question was placed in the survey to establish whether the board, the executive or the functional arrangements might correlate with the maturity of ERM in leading Australian companies. The graphical and descriptive analysis, supported by the survey comments, tell an interesting story.

The following Figure 4.12 shows the distribution of S&P/ASX 200 companies surveyed across the five point Likert scale outlined above. The companies on the left, at scale point one have very little association with ERM. Those across to the right, have more well developed, mature ERM systems and processes.
Figure 4.12  Adoption of ERM by S&P/ASX 200 companies

Figure 4.12 shows that eighty eight percent of the S&P/ASX 200 companies are in the categories from three to five on the Likert scale. These leading Australian companies are familiar with ERM, are progressing down a pathway of implementation and are increasing their ERM maturity. This confirms the fact that ERM is becoming a leading consideration in the Australian business fabric.

Earlier, writers such as Subramaniam et al (2009), Ruigrok et al (2006) and Benz and Frey (2007) referred to agency theory in relation to company size. They predicted that larger companies would have some form of risk management presence. The size of the company is related to the level of resources that can be directed towards agency arrangements such as board committees. Size is also related to political visibility, which also incurs costs. Larger companies have a higher potential for government scrutiny and interference.

With regard to ERM, the agency theory related factors of size and industry classification tell a story. The following figure outlines the average revenue for the companies surveyed in each of the above five Likert scale categories.
The average revenues in Likert categories three, four and five are above the overall average for the S&P/ASX 200 companies. It therefore appears that the maturity of ERM implementation may be related to the agency cost factor of company size. This supports the findings of the Subramaniam et al (2009) and Beasley et al (2005) studies, noted in Chapter Two, that found a positive relationship between entity size and the adoption of risk management through ERM or a dedicated risk committee.

Figure 4.14 highlights the average score on the Likert scale for the one hundred and two survey respondents classified by GICS category. This figure shows whether any particular GICS category is leading or lagging in ERM implementation:
<table>
<thead>
<tr>
<th>GICS CATEGORY</th>
<th>AVERAGE LIKERT SCORE</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 Energy</td>
<td>3.5</td>
</tr>
<tr>
<td>15 Materials</td>
<td>3.5</td>
</tr>
<tr>
<td>20 Industrial</td>
<td>3.4</td>
</tr>
<tr>
<td>25 Consumer Discretionary</td>
<td>3.6</td>
</tr>
<tr>
<td>30 Consumer Staples</td>
<td>2.8</td>
</tr>
<tr>
<td>35 Health</td>
<td>3.5</td>
</tr>
<tr>
<td>40 Financial</td>
<td>3.6</td>
</tr>
<tr>
<td>45 Information Technology</td>
<td>4.0</td>
</tr>
<tr>
<td>50 Telecommunications</td>
<td>2.5</td>
</tr>
<tr>
<td>55 Utilities</td>
<td>3.8</td>
</tr>
<tr>
<td>All survey respondents</td>
<td>3.5</td>
</tr>
</tbody>
</table>

**Figure 4.14  Average Likert score for S&P/ASX 200 companies by GICS**

The Likert scale average for each GICS category ranges from 2.8 to 4.0, with the overall average being 3.5. The outliers, being consumer staples at 2.8 and telecommunications at 2.5, had very small numbers of survey participants which may have skewed the averages. Overall the state of ERM preparedness across the S&P/ASX 200 is similar between GICS categories and there does not seem to be any industry grouping that is leading in or falling behind on ERM adoption.

To the author’s knowledge, this is the first time that an examination of the self reported maturity of ERM development in the S&P/ASX 200 companies has been attempted.

Overall, Australian S&P/ASX 200 companies, who responded to the survey were aware of ERM and the majority self reported that they are well progressed with ERM adoption.
Adoption appears more advanced in the larger Australian companies. There is no particular industry segment that stands out as leading in the adoption of ERM. This finding aligns with the overseas work of Kleffner et al (2003), Colquitt et al (1999) and Beasley et al (2005). Those studies found that the maturity of ERM is positively related to company size. It would appear that larger companies have the resources at board level, an agency cost perspective, to fully implement ERM. Signalling theory would also suggest that the larger, more visible companies, owned by institutional investors, and subject to S&P ratings, would benefit from a well publicised ERM process.

This finding addresses the first research objective on the structural arrangements for risk management in Australian leading companies. ERM implementation was a second order driver for a portion of the 17% of companies that have a separate board risk committee. ERM was not identified as a primary driver for the 73% of S&P/ASX 200 companies that have a combined board audit and risk committee. It appears that ERM implementation is not a major driver behind the structure of risk management in the S&P/ASX 200.

Next, executive oversight is examined to ascertain what systems of governance the S&P/ASX 200 companies are placing over risk management below board level.

4.9 EXECUTIVE MANAGEMENT OVERSIGHT OF RISK

Chapter Two introduced the CRO and revealed that internationally both the CRO and the CFO may take an executive role in the governance of risk management. Tillinghast-Towers Perrin and IIA (2001) reported that 30% of international organisations now have a CRO. Deloitte (2004) reported that 81% of international financial services companies have a CRO. This section looks at the executive management over risk in leading Australian companies. The research objective of explaining how the CRO fits into the Australian business structure is addressed.
The desk-top analysis could not draw any conclusions below the board level of management. In the S&P/ASX 200 annual reports, companies are not required to outline executive positions or management structure.

Survey question seven (see Appendix Three) asked: Which executive officer is responsible for risk management at the operational level? The results of the survey of S&P/ASX 200 companies are outlined in Figure 4.15 below. The findings show that in Australia, the CFO is the senior executive most likely to oversee risk management.

*Figure 4.15 Executive oversight of risk management in S&P/ASX 200 companies. A sample of 102 observations from a population of 200 which at the 95% confidence level gives a confidence interval of +/- 7%*

The survey results show that 32% of S&P / ASX companies have risk management reporting to the CFO, 26% to a CRO and 19% to the CEO. Interestingly, 9% of these companies have risk management under the CAE, another indication of the growing integration between internal audit and risk management. These reporting arrangements to different executives, also support the diversity in CRO job descriptions as discussed by Ernst and Young (2007).
These findings also align with the international picture as portrayed by Tillinghast-Towers Perrin (2001). That study found that only 30% of organisations have a CRO.

The companies were split by GICS, to determine which officer was the senior risk executive, by industry, in the S&P/ASX 200 companies. This sorting was designed to uncover any contingency or environmental aspects to the appointment of a CRO. Figure 4.16 outlines that spread:

<table>
<thead>
<tr>
<th>Survey – Companies by GICS</th>
<th>Number of Companies</th>
<th>CRO %</th>
<th>CFO %</th>
<th>OTHER %</th>
<th>TOTAL %</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 - Energy</td>
<td>6</td>
<td>50%</td>
<td>33%</td>
<td>17%</td>
<td>100%</td>
</tr>
<tr>
<td>15 - Materials</td>
<td>12</td>
<td>17%</td>
<td>42%</td>
<td>42%</td>
<td>100%</td>
</tr>
<tr>
<td>20 - Industrials</td>
<td>25</td>
<td>32%</td>
<td>32%</td>
<td>36%</td>
<td>100%</td>
</tr>
<tr>
<td>25 &amp; 30 - Consumer</td>
<td>21</td>
<td>14%</td>
<td>43%</td>
<td>43%</td>
<td>100%</td>
</tr>
<tr>
<td>35 - Health</td>
<td>5</td>
<td>20%</td>
<td>20%</td>
<td>60%</td>
<td>100%</td>
</tr>
<tr>
<td>40 - Financial</td>
<td>22</td>
<td>36%</td>
<td>27%</td>
<td>36%</td>
<td>100%</td>
</tr>
<tr>
<td>45 &amp; 50 – IT and Telecoms</td>
<td>2</td>
<td>50%</td>
<td>0%</td>
<td>50%</td>
<td>100%</td>
</tr>
<tr>
<td>55 - Utilities</td>
<td>9</td>
<td>22%</td>
<td>11%</td>
<td>67%</td>
<td>100%</td>
</tr>
<tr>
<td>TOTAL</td>
<td>102</td>
<td>26%</td>
<td>32%</td>
<td>42%</td>
<td>100%</td>
</tr>
</tbody>
</table>

**Figure 4.16 Executive management oversight of risk in the S&P/ASX 200 by GICS**

To determine whether the values of the survey sample in Figure 4.16 are statistically significant with regard to the population, a Chi Square test was completed and resulted in the following outputs:
<table>
<thead>
<tr>
<th>GICS</th>
<th>Classification</th>
<th>Sample</th>
<th>Chi Square</th>
<th>X Squared</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Energy</td>
<td>6</td>
<td>1.00</td>
<td>5.991</td>
</tr>
<tr>
<td>15</td>
<td>Materials</td>
<td>12</td>
<td>2.00</td>
<td>5.991</td>
</tr>
<tr>
<td>20</td>
<td>Industrials</td>
<td>25</td>
<td>0.31</td>
<td>5.991</td>
</tr>
<tr>
<td>25</td>
<td>Consumer Disc</td>
<td>14</td>
<td>4.00</td>
<td>5.991</td>
</tr>
<tr>
<td>30</td>
<td>Consumer Staples</td>
<td>7</td>
<td>1.60</td>
<td>5.991</td>
</tr>
<tr>
<td>35</td>
<td>Health</td>
<td>5</td>
<td>0.50</td>
<td>5.991</td>
</tr>
<tr>
<td>40</td>
<td>Financial</td>
<td>22</td>
<td>0.36</td>
<td>5.991</td>
</tr>
<tr>
<td>45</td>
<td>IT</td>
<td>1</td>
<td>0.36</td>
<td>5.991</td>
</tr>
<tr>
<td>50</td>
<td>Telecoms</td>
<td>1</td>
<td>2.00</td>
<td>5.991</td>
</tr>
<tr>
<td>55</td>
<td>Utilities</td>
<td>9</td>
<td>4.67</td>
<td>5.991</td>
</tr>
</tbody>
</table>

**Figure 4.17 Chi Square statistical significance results for Figure 4.16**

From a statistical table (Hanneman, Kposowa and Riddle, 2012) at alpha = 0.05, and 2 degrees of freedom, the critical value of $X^2$ squared is 5.991.

Since all the Chi Square values for each bracket of three variables (CRO, CFO & Other) are < 5.991, the null hypothesis cannot be rejected, therefore the sample is statistically representative of the population, for all GICS categories, at the 0.05 level of significance.

From the 102 surveys received, the second column in Figure 4.16 shows the number of companies in each GICS category. The next three columns show the percentage by GICS for each of the companies with the CRO, CFO, or other officer as the lead risk management executive.
Figure 4.16 clearly shows that for the energy sector (GICS 10), the financial sector (GICS 40) and the IT and telecommunications sectors (GICS 45 and 50) the CRO has overtaken the CFO as the leading executive over risk management. However, care should be taken with the findings for GICS 45 and 50 due to the small number of respondents in these survey categories.

The above finding aligns with the Liebenberg and Hoyt (2003) study in the United States and the Kleffner et al (2003) Canadian study. Both these studies found a greater use of CRO’s in the energy and finance sectors. It appears that in these sectors the CRO is able to contribute to the executive team. The finding that the CRO is the lead risk executive in the GICS 40, financial sector, also supports the Deloitte (2004) global survey finding where 81% of international financial services companies have a CRO. This may be an example of mimetic isomorphism, where Australian companies are copying international good practices.

Having CROs control risk management in the energy and financial sectors may not be surprising. Both these sectors use financial derivatives to hedge spot market transactions. The energy sector uses electricity and gas derivatives, the financial sector uses interest rate and foreign currency swaps. Poor risk management involving the use of these derivatives can lead to huge losses, for example Societe Generale S.A. (Euro 4.9 billion), NAB (A$360 million) and Pacific Power (A$300 million). In these sectors the CRO has a very large responsibility. As suggested by Meyer and Rowan (1977), the appointment of a CRO as a signalling device might legitimise the risk management activities of that institution and ensure continued financing and support from the markets.

In a similar vein, the appointment of a CRO might signal mitigation to the Fama and Jensen (1983) risk shifting problem. Lenders know that shareholders can alter the firms risk profile after debt has been secured.
The appointment of a CRO in the higher risk energy and banking environments might signal a commitment to preventing risk shifting behaviour. This would reduce information asymmetry between stakeholders and the company.

The interviews provided support for the above findings. One banking sector executive commented on some institutional theory factors around the appointment of a CRO:

_In the global investment banks the CRO is very powerful. He would have legal, tax, compliance, operational risk and audit reporting through to him and would have the power to veto transactions. In Australia this model exists but is only starting to take hold. (COSEC from a GICS 40 company)_

Another executive responded that:

_The merging of risk management and internal audit under a single executive has become the industry standard. The roles being advertised at the top level are now called Director of Risk or Chief Risk Officer. (CRO from a GICS 50 company)_

Another related fact emerged from the responses to question twelve in the survey. It appears that when a company outsources its internal audit function, the CFO or CRO often manage the contractual relationship and work program for the outsourced auditor. Four executives noted:

_One of our executives is both the CRO and Company Secretary. He manages the outsourced internal audit contract. (COSEC from a GICS 40 company)_

_The outsourced internal audit function reports through to the audit committee. The CFO liaises with the internal auditors and manages them. (COSEC from a GICS 40 company)_

_The outsourced internal audit is managed by the Head of Risk. (COSEC from a GICS 40 company)_
The CRO also manages the internal audit outsourcing arrangement. (COSEC from a GICS 20 company)

This aspect is further discussed in Section 4.11 below.

Across all S&P/ASX 200 companies, the CFO is still the leading executive overseeing risk management. However, the CRO has taken over as the prime risk executive in the energy, information technology, telecommunications and financial services sectors. This may be driven by contingency theory where the activities in the energy and financial sectors include hedging using complex financial derivatives. A specialised CRO with unique “middle office” skills may be more appropriate than a more generalist CFO. Alternatively, as was found in the Liebenberg and Hoyt (2003) study, firms may appoint CROs to reduce information asymmetry relating to the firms risk profile. This could be underpinned by signalling theory.

The above finding helps resolve another aspect of the first research objective on the risk management structure at executive levels in Australia.

The next section moves down to the functional level and seeks to understand the governance oversight of risk management at the operational level. The integration between internal audit and risk management is also considered.

4.10 INTEGRATION AT THE FUNCTIONAL LEVEL

One of the research objectives for this study was to explore the levels of integration between internal audit and risk management in leading Australian companies. Previous literature, such as McNamee and Selim (1998) and Walker, et al (2002) has addressed aspects of integration between internal audit and risk management.
At the functional level the desk-top analysis failed to assist. Useful information, below the executive level, could not be accessed from either annual reports or from the corporate governance statements provided by the companies. The survey of S&P/ASX 200 companies provided much of this information.

Question eight in the survey (see Appendix Three) asked about the arrangements for risk management at the functional level. The following Figure 4.18 outlines the results of the survey.

**Figure 4.18** Separation of internal audit and risk management at the functional level in the S&P/ASX 200 companies. A sample of 102 observations from a population of 200 which at the 95% confidence level gives a confidence interval of +/- 7%

Thirty percent of survey respondents reported that they had combined internal audit and risk management at the functional level. This aligns with the PWC (2007) United States survey that found one third of internal auditors are responsible for the ERM function in their organisation.

Fifty six percent of respondents indicated that they had a separate risk function to the internal audit function. Two percent indicated that they had outsourced risk management and 12% of respondents reported that they had no risk management function.
The percentage of respondents that reported a separated functional arrangement was high. The problem uncovered was that many of these respondents had reported a separated function, when in fact the internal audit and risk management functions reported to the same executive. This raised a dilemma over the definition of a separated internal audit and risk management function. If internal audit and risk management both report through to the same executive, usually the CFO or CRO, are the functions really separated? Unfortunately the survey questions were not drafted in a manner that captured this dual reporting relationship. However the interview questions, which were designed after the survey responses were received, were able to be structured to capture more of this information.

To investigate this dilemma further, the interviews with company executives were examined. Thirty five interviewees provided organisational charts that outlined the reporting structure for internal audit and risk management within their organisation. A copy of one of these organisational charts is attached as Appendix Thirteen. At this stage it should be noted that the interviews cannot be fully representative of the full S&P/ASX 200 population due to the small number of interviews.

The following figure compares the responses from the one hundred and two survey responses to the thirty five responses from the interviews. It can be seen that the interview sub-set is consistent with the survey percentages:
<table>
<thead>
<tr>
<th>Internal Audit / Risk Management Functional Model</th>
<th>Survey Respondents</th>
<th>Interviews Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comparison of Survey to Interviews</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Combined</td>
<td>30%</td>
<td>35%</td>
</tr>
<tr>
<td>Separated</td>
<td>56%</td>
<td>59%</td>
</tr>
<tr>
<td>Outsourced RM</td>
<td>2%</td>
<td>0%</td>
</tr>
<tr>
<td>Other (includes no risk or audit)</td>
<td>12%</td>
<td>6%</td>
</tr>
<tr>
<td>TOTAL</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

**Figure 4.19** Comparison of survey responses to interview responses in the S&P/ASX 200 companies

In the interviews 20 respondents stated that their internal audit and risk management functions were separated. That is the 59% outlined above. From that group of twenty interviewees, thirteen, or more than half, reported that their internal audit and risk management reported to a single executive. Therefore, using a conservative estimate, up to half of those companies in Figure 4.16 which reported separated audit and risk functions (56%) may have internal audit and risk management reporting to the same executive.

On the question of whether having internal audit and risk management reporting through to the same executive constitutes integration between audit and risk, a consumer discretionary executive provided the following insight:

*The rationale for having internal audit and risk management separated is nonsense. In most cases the separated internal audit and risk management both report to the CFO, thereby destroying any independence. (COSEC from a GICS 25 company)*

The above comment also supports the Christopher et al (2009) finding that organisations often operate in an environment that compromises audit independence.
There is strong evidence of integration with 30% of survey respondents reporting that they had combined their internal audit and risk management at the functional level. From the above calculations at least another 25% may have both functions reporting through to the same executive, thereby adding further weight to the integration argument. If combined, over 50% of S&P/ASX 200 Australian companies show some level of integration at the functional level. These findings are consistent with the levels of integration outlined by Leung et al (2004), Goodwin-Stewart and Kent (2006) and Spira and Page (2002).

Two percent of respondents reported that they had outsourced risk management and 12% stated that they had no centralised risk management function. An executive from a property trust stated:

_We are very small and lean. The board and key executives meet to review risks as a team. The compliance manager is in some senses a risk manager._ (COSEC from a GICS 40 company)

Again, the size of the company may be an agency related factor where risk management is absent. Smaller companies may not be able to afford both internal audit and risk management functions. Subramaniam et al (2009) found that the existence of risk committees increased with the agency related factor of company size.

It can be estimated that approximately a quarter (half the 56% in figure 4.14) of S&P/ASX 200 companies have a strict separation of the internal audit function from the risk management function. By strict separation, the functions are distinctly separate and each function reports to a different executive.
4.10.1 Reasons for Integration between Internal Audit and Risk Management at the Functional Level

Question ten in the survey (see Appendix Three) asked the respondents for the reasons why they had integrated internal audit and risk management at the functional level.

The question outlined five reasons for choosing an integrated team with space on the survey for additional comments if necessary. The five reasons were derived from pilot interviews before the survey was undertaken and from the prior research in Chapter Two. The choices were ranked on a five point Likert scale, ranging from not important through to very important. The choices consisted of:

1. to save costs;
2. both audit and risk are internal controls;
3. this is the industry standard model;
4. the company is too small to have separate functions; and
5. natural synergies between audit and risk.

Figure 4.20 Reasons for integrating audit and risk in the S&P/ASX 200 companies
Figure 4.20 outlines the results of the survey. The two most significant factors are that internal audit and risk management are both internal controls and have strong synergies. To better understand whether the synergies seen at the functional level align with those at the board committee level we can turn to comments from the survey respondents.

Four executives provided comments that help clarify the importance of these synergies:

The synergies between risk and assurance deliver a broad overview of the risk profile to the board and the executive. (Executive from a GICS 30 company)

Combining internal audit and risk management enhances the understanding of the business and how risks are managed plus helps foster a culture of risk management at the operational level. (COSEC from a GICS 15 company)

We are merging internal audit and risk management, which is the next logical step. As long as you allow the auditor a direct line to the audit committee, there is no independence problem with merging. (CRO from a GICS 40 company)

To ensure that the status of organisational risks, and management’s ability to address them, is presented as a single and aligned story. Also to ensure that audit resources are focussed on addressing controls related to the most significant risks. (Executive from a GICS 50 company)

Finally, another telecommunications company saw integration as a way to “kick start” the implementation of ERM:

The risk management methodology, framework and tools were developed by internal audit, who also provide training and on-line modules for staff capability development. (CRO from a GICS 50 company)
The next section considered whether those with integrated internal audit and risk management functions saw independence as an issue.

### 4.10.2 Integration and Independence

In Chapter Two the independence concerns with respect to the integration of internal audit and risk management were outlined. IIA professional standard number 1100 requires internal auditors to be “independent and objective” in performing their work. A question then arises: How do companies that have integrated internal audit and risk management handle the independence issue?

Survey question eleven (see Appendix Three) asked the 30% of respondents, with integrated internal audit and risk management, what concerns they had with the audit independence issue. The outcome is presented in Figure 4.21 below:

![Figure 4.21](image)

**Figure 4.21** Independence concerns for integrated risk and audit teams in the S&P/ASX 200 companies. A sample of 102 observations from a population of 200 which at the 95% confidence level gives a confidence interval of +/- 7%

Figure 4.21 indicates that companies with integrated internal audit and risk management functions generally did not see independence as an issue. The comments provided in the surveys help to understand this finding.
One financial company executive stated:

*Although we have risk, compliance and legal in with internal audit, we don’t have any independence issues. The head of audit has a dotted line to the board audit committee.* (COSEC from a GICS 40 company)

For those who did acknowledge independence concerns, 35% handled this by outsourcing the audit of risk management related audits, and 4% set up “Chinese Walls” within the combined audit and risk team. Chinese walls are a set of processes put in place to keep internal departments effectively separate.

Having internal audit outsourced may help alleviate independence concerns. A bank and a consumer staples executive commented:

*Although both the internal audit and risk management functions report to the company secretary, independence is maintained by the outsourcing of internal audit.* (COSEC from a GICS 40 company)

*We do not have any independence issues because although the same executive looks after audit and risk, audit is outsourced to a “Big Four” company.* (CRO from a GICS 30 company)

However, as outlined in Chapter Two, concern over independence is still the primary driver for keeping the internal audit and risk management functions separated. This is confirmed in the next section, where survey respondents who reported separate risk and audit functions, cited independence as the main driver for separation. Later in this Chapter a similar theme emerged from interviews with respondents.

**4.10.3 Separated Functional Teams**

Figure 4.18 above shows that 56% of S&P /ASX 200 companies keep their internal audit and risk management functions separated.
Question nine in the survey (see Appendix Three) asked those respondents why a separated model had been chosen. The question gave six alternatives to be ranked on a five point Likert scale, ranging from not important through to very important. The alternatives were:

1. internal audit is outsourced;
2. independence;
3. no links between internal audit and risk management;
4. another executive (not the CAE) has accepted responsibility for risk management;
5. because there is a separate risk committee at board level; and
6. no reason; evolved over time.

Figure 4.22 outlines the results of question nine of the survey:

![Chart showing reasons for separating internal audit from risk management in the S&P/ASX 200 companies.]

Figure 4.22  Reasons for separating internal audit from risk management in the S&P/ASX 200 companies

Clearly, the most significant factor was the requirement to keep internal audit separated from risk management for independence reasons. This is consistent with the IIA international standard and Christopher et al (2009) position. Both the IIA and the Christopher et al (2009) study strongly recommended that internal audit must be independent.
A lesser but marginally significant factor is having an executive officer, other than the CAE, available to take responsibility for risk management.

The independence issue became focused in the comments made by respondents to the survey:

*Internal audit must be independent (from risk management) to undertake reviews of risk assessment and mitigations. (A CAE from a GICS 40 company)*

*We have recently separated the internal audit and risk management functions. Internal audit is seen as a mechanism for validation of controls, for example, confirmation of risk ratings. (CFO from a GICS 30 Company)*

APRA regulation may also play a role. One insurance company advised that:

*We have a regulatory requirement to have the risk function independently audited, and in our view the maker of the framework cannot check the framework elements. (COSEC from a GICS 40 company)*

There may be too much focus on the traditional independence view now that risk management has become more prominent. In an organisation where internal audit has evolved from a compliance role to a partnership role, the benefits from having the internal auditors, who are trained in risk and control assessment, working with management to deliver solution’s might outweigh the independence concerns. This is consistent with a knowledge management view. Using the tools of risk management and internal audit and the common languages, those professionals can work together to convert difficult tacit issues into understandable explicit knowledge.

As long as the head of internal audit can discuss issues with the audit committee, there may be no serious independence issues with integration. This issue is further explored in the interviews and in the models developed later in this chapter.
Full integration between internal audit and risk management is occurring in 30% of companies where respondents stated that risk management is now combined with internal audit. These companies see the synergy between audit and risk outweighing concerns regarding independence at the operational level.

For those companies who had combined risk and audit teams, the majority did not see independence as an issue. For the small number who had independence concerns, they either outsourced the auditing of risk management or established internal “Chinese walls”.

The study found that 30% of S&P/ASX 200 companies had integrated risk management and internal audit. Another 30% used a partially integrated model where, although risk and audit are in separate teams, both teams report to a single executive. Fourteen percent either outsource risk management or have no risk management function.

The remaining S&P/ASX 200 companies (approximately 25%) have internal audit separated from risk management at the operational level, primarily due to traditional audit independence concerns.

The above finding goes towards meeting research objective two, establishing the levels of integration between internal audit and risk management in leading Australian companies. Over half of the two hundred companies included in this research had exhibited some level of integration. This means companies can combine their internal audit and risk management teams to save costs and capture the full benefits of synergy, through knowledge management.

4.11 OUTSOURCING OF INTERNAL AUDIT

Due to the debate over the relationship between risk management and internal audit, the internal audit arrangements for each S&P/ASX 200 company was investigated. Whether internal audit is outsourced or remains in-house may impact on the structure of risk management.
Earlier it was reported that some S&P/ASX 200 companies overcame the independence issue by outsourcing internal audit, but still have internal audit and risk management oversight by a single executive.

Carey et al (2006) found a positive relationship existed between the presence of internal audit arrangements and the revenues of companies. This finding aligns with the work outlined by Goodwin-Stewart and Kent (2006). Martin and Lavine (2000) found that agency cost is a factor in outsourcing internal audit. Larger companies can afford to co-source internal audit, a combination of internal and outsourced resources, whereas small companies might prefer to outsource these agency controls for budgetary reasons.

Question twelve in the survey (see Appendix Three) asked respondents to outline the internal audit arrangements in their company. They had a choice of co-sourcing, outsourcing or no internal audit function. The following figure shows the results for the S&P/ASX 200 population:

![Figure 4.23](image)

**Figure 4.23** Levels of co-sourcing and outsourcing in the S&P/ASX 200 companies. A sample of 102 observations from a population of 200 which at the 95% confidence level gives a confidence interval of +/- 7%.

They found that only 34% of companies had an internal audit function and 25% of that 34% were outsourced. Only 8% of the entire population of 450 companies studied had an outsourced internal audit function.

Carey et al (2006) in a similar study completed in 1998 found that 33% of companies had an internal audit presence and within this group 20% were outsourced. This translates to 7% of those companies in the study having outsourced internal audit.

As shown in Chapter Two, a survey of S&P/ASX 200 companies conducted by Regnan GRE in 2008 found 79% of S&P/ASX 200 companies had an internal audit function.

The following table compares the above studies with this research:

<table>
<thead>
<tr>
<th>Author</th>
<th>Year</th>
<th>Population</th>
<th>Internal Audit %</th>
<th>Outsourced %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carey et al (2006)</td>
<td>1998</td>
<td>All ASX listed companies, 304 survey responses</td>
<td>33%</td>
<td>20% of those with internal audit; 7% of population</td>
</tr>
<tr>
<td>Goodwin Stewart &amp; Kent (2006)</td>
<td>2000</td>
<td>All ASX listed companies, 450 survey responses</td>
<td>34%</td>
<td>25% of those with internal audit: 8% of population</td>
</tr>
<tr>
<td>Regnan GRE</td>
<td>2008</td>
<td>S&amp;P/ASX 200</td>
<td>79%</td>
<td>Not surveyed</td>
</tr>
<tr>
<td>Halliday (2012)</td>
<td>2008</td>
<td>S&amp;P/ASX 200 companies, 102 responses</td>
<td>82%</td>
<td>30% of those with internal audit: 25% of the population</td>
</tr>
</tbody>
</table>

**Figure 4.24 Internal audit and outsourcing comparisons**
The above research has different populations and therefore comparisons cannot be validly made between outcomes. However, the table shows that the S&P/ASX 200 companies today are more likely to have an internal audit function than the wider population of all Australian companies approximately a decade earlier. The S&P/ASX 200 companies are the more economically significant companies and have greater resources to implement internal audit. Because of their size, they are also the companies that are more likely to suffer political scrutiny and are therefore signalling good governance by having an internal audit function. In addition, the ASX Principles, which were first published in 2003, now require an audit committee. The requirement to set up an audit committee may in turn put pressure on the adoption of internal audit functions to support that committee.

The above table suggests that outsourcing may be increasing however the populations are not the same which limits the validity of such a claim. An increase to the amount of outsourcing has some practical appeal. With the arrival of risk management and the CRO, outsourcing is a valid way to have risk management as the central function, while still allowing for compliance audits by an outsourced provider, without impacting on independence. The CRO and risk function can be forward looking strategic partners with management, while compliance audits by an outsourced provider complete the third line of defence.

The survey did not ask a question on why internal audit was outsourced. That research question has been well researched previously. However, the comments from respondents on question twelve in the survey (see Appendix Three) shed some light on this issue.

Firstly, the study found that when internal audit is outsourced, often an in-house executive has control over management of the contractor:
The outsourced function reports to the audit committee. The CFO liaises with the contractor from the management team. (CFO from a GICS 40 company)

One executive is CRO, Company Secretary and manages the outsourced internal audit contract. (COSEC from a GICS 40 company)

Outsourced internal audit function is managed by the head of risk. (CRO from a GICS 40 company)

We saw a real benefit in appointing an external internal audit function. These external contractors bring real experience from the industry. It is important for management to see independence in the function and the ability to report separately and directly to the board committee. (COSEC from a GICS 40 company)

The internal audit team is outsourced, but structured in such a way as to be considered an internal resource through the risk management function. (CRO from a GICS 25 company)

This perhaps raises a definitional dilemma. If internal audit is outsourced, but an internal executive oversees that function, surely the arrangement becomes co-sourced, or a mix of internal and external resources. At the limit, one could argue that there is no such thing as outsourcing, only different degrees of co-sourcing.

Figure 4.23 shows that co-sourcing internal audit is the arrangement of choice in the S&P/ASX 200 population. Co-sourcing involves a blend of internal and external resources, often using contractors to supplement in specialised areas or when in-house resources are scarce.

The comments from respondents on the issue of co-sourcing help clarify the rationale for such a blending of experience:
Our CAE reports to the CFO and engages external resources where necessary. (CFO from a GICS 35 company)

An in-house team managed by a CAE with some co-sourcing to access specialist skills. (CAE from a GICS 25 company)

Co-sourcing with external providers is for specialist areas only – a small percentage of total activity. (CRO from a GICS 40 company)

Our governance is internally coordinated using external consultants, the risk manager or the internal auditors to conduct reviews. The determination of approach is based on: 1) the need for independence; 2) the need to build internal commitment; or 3) the need to leverage off skills. (COSEC from a GICS 40 company)

Finally, the size of S&P/ASX 200 companies surveyed was investigated in the context of whether they had co-sourced, outsourced or had no internal audit function. The following table highlights those results, which are based on the average revenue of companies falling into each category:

<table>
<thead>
<tr>
<th>Functional Model</th>
<th>All S&amp;P/ASX 200</th>
<th>Co-sourced</th>
<th>Outsourced</th>
<th>No Internal Audit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average Revenue</td>
<td>$3,443</td>
<td>$3,743</td>
<td>$596</td>
<td>$142</td>
</tr>
</tbody>
</table>

Figure 4.25 Average revenue for outsourced and co-sourced internal audit in the S&P/ASX 200 companies

Clearly the co-sourced internal audit functions reside within the larger S&P/ASX 200 companies. Earlier, agency theory was discussed in terms of its relationship with company size, as suggested by Subramaniam et al (2009). In line with agency theory, these outsourced arrangements appear centred around smaller companies. The “no internal audit” companies are even smaller based on revenue.
This aligns with previous findings that smaller, perhaps recently incorporated and less mature companies, such as mining start-up companies, may be implementing outsourced internal audit as a first step in their governance process. The notion of company size and outsourcing, in particular when internal audit is first considered, was raised by Carey et al in 2006. That study concluded that small firms, when introducing internal audit, outsource as a first step.

The research found that 82% of S&P/ASX 200 companies have some form of internal audit function. This is a large increase over the findings in earlier research, which concentrated on a larger population of Australian companies. Thirty percent of companies outsource internal audit and 57% have a co-sourced arrangement. The co-sourced model usually has an in-house executive controlling the outsourcing arrangements, often through the CRO. With the co-sourced arrangement having average revenues above the S&P/ASX 200 average co-sourcing appears to be positively related to the size of the company.

The above finding helps clarify research objective one, to investigate how risk management is structured in the S&P/ASX 200 companies. It seems that 30% of leading companies outsource internal audit and have that outsourced function report to a senior executive. It would be easy to add this role to the CRO, thereby gaining leverage from the synergies between internal audit and risk management.

4.12 NO INTERNAL AUDIT

Goodwin-Stewart and Kent (2006) and Carey et al (2006), both found that only one third of Australian companies have an internal audit function. The previous section of this research found that in the S&P/ASX 200 companies the percentage having an internal audit function is 82%. However there are still 18% of leading Australian companies without any internal audit presence.
Goodwin-Stewart and Kent (2006) found a strong relationship between the internal audit arrangements and company revenue. The next section explores this relationship further.

4.12.1 Revenues

The average revenue for all S&P/ASX 200 companies, taken from the full population, desk-top analysis is $3,443 million. The eighteen companies who responded in the survey that they had no internal audit function had on average revenue of only $142 million. This observation indicates that the agency related factor of company size may influence the decision to adopt an internal audit function. Start up mining companies, for example, may be too early in their life cycle to adopt an internal audit presence.

4.12.2 Industry Classification

Using GICS as a differentiator the following figure reinforces the relationship between internal audit and company size:

![Figure 4.26 S&P/ASX 200 companies with no internal audit by GICS. A sample of 102 observations from a population of 200 which at the 95% confidence level gives a confidence interval of +/- 7%](image-url)
The materials and energy sector jointly comprise 61% of the smaller companies with no internal audit function. A review of the survey respondents found that these sectors include the smaller mining and petroleum exploration companies.

4.12.3 Interviews with No Internal Audit Companies

To better understand the drivers for having no internal audit function, the author contacted all eighteen survey respondent companies, by email, seeking comments on why no internal audit function existed. Five responses were received and can be categorised into four broad categories:

1. **We are new and not yet ready.** For these smaller, less mature companies, the governance had not yet evolved to the extent that an internal audit function was adopted.

   *We are a young company and the board is just getting on top of risk management through the audit committee. The audit committee looks after business and commercial interests, which align with risk management.* (A COSEC from a GICS 15 company)

2. **Internal audit is not required by ASX.** This is premised on the ASX Principles, while requiring an audit committee do not mandate an internal audit function. One communications company commented:

   *We align with ASX Principles which require a risk management presence but do not require any internal audit.* (CRO from a GICS 50 company)

   This is an interesting finding for both the internal audit and risk management professional institutions. The IIA, in Australia has been vocal over recent years about the need to legislatively mandate for an internal audit function.
The risk management profession, on the other hand, see the failure to mandate internal audit as an opportunity for risk management to broaden its role in Australian companies.

3. **Parent has internal audit.** This rationale arises where an Australian ASX company has an overseas parent, perhaps regulated by SOX, who has a comprehensive internal audit function:

   *We are consolidated with our parent company and are required to be Sarbanes Oxley compliant. This sets a very high bar for internal review which is provided by the parent.* (CRO from a GICS 40 company)

4. **De-facto internal audit.** Two of the respondents conducted internal audit style reviews under another guise. Risk management, compliance, peer review and continual improvement functions provided a surrogate internal audit role. An executive from a property trust noted:

   *We do not ask experts to come in and identify issues that we already know about. Risk is the initiator and our de-facto audit (continuous improvement) is the fixer. This is a mature and well advanced approach, possibly the way for the future.* (CRO from a GICS 40 company)

Both of the interviewees quoted in point four above commented that they would not use the term “internal auditor” because of the negative connotations associated with that term.

Point four above has significant ramifications for the auditing profession. The integration of internal audit into existing or new governance roles has the potential to be a future direction, perhaps a paradigm change in Australian companies. Cooper et al (2006) reported that in Australia, top management are generally unsupportive of internal audit. Management may look to other governance sources to add such value.
As the firm evolves the continual improvement, business development, sustainability or risk management function may take on the role of internal auditor. A dogged fixation on independence may keep internal audit out of mainstream strategy and decision making. Management may switch across to the more “management friendly” risk management function for assistance in making strategic decisions and recommend the actions to mitigate associated risks. This issue is covered in greater depth in the final sections of this chapter where the interview responses help develop models for governance over risk management.

In summary, 18% of the S&P/ASX 200 leading Australian companies have no internal audit function. These tend to be smaller companies and largely in the material sector, which includes start-up mining and petroleum exploration companies. Interviews with a number of companies revealed that some of the more established have a de-facto internal audit function residing within the risk management or continual improvement areas. This finding indicates a move away from traditional internal audit in favour of risk management or continual improvement functions. This finding therefore has the potential to take the literature in a completely new direction. If the value from leveraging on knowledge management by using risk managers as internal auditors outweighs independence concerns, then this presents a new paradigm to the internal audit profession.

Up to this point in the research findings reliance has been placed on the desk-top analysis, the survey outcomes and comments from respondents to the survey. Quotes from the interviewees have been used where pertinent, but lightly. These findings are therefore based on the quantitative end of the research spectrum.

Interviews were also conducted with thirty five executives from S&P/ASX companies. In addition, four interviews were held with risk management partners in each of the “Big Four” companies.
These interviews provide a more qualitative aspect to the research, a synthesis of the thoughts and understanding of the executives working in the area of risk management.

4.13 INTERVIEWS WITH EXECUTIVES

Before continuing, a note of caution needs to be stated. The earlier desk-top analysis and survey work are both accurate and reliable. The desk-top analysis provided accurate and verifiable information from publicly available sources on 100% of the population of S&P/ASX 200 companies. The survey achieved a 59% response rate which was unusually high for this type of research. The author is therefore confident that the desk-top and survey analyses are broadly representative of the whole population within the S&P/ASX 200 companies.

This section looks at qualitative findings from thirty nine interviewees. Those interviewees are not statistically representative of the whole population (Eriksson and Kovalainen, 2008). Those who agreed to be interviewed could, for example, be the more out-spoken or more controversial risk executives. We cannot say that these interviews are free from bias or are entirely representative of the population. However the interviews were rich in the level of information provided, and must be included in the research outcomes.

The author does feel however, that these interviews are broadly representative of the population because the executives interviewed grouped into the same governance groupings that were represented in the survey. For example, 30% of survey respondents advised that they had combined their risk and audit functions at the operational level. Thirty five percent of interviewees said the same. The interviews matched the survey groups which indicates that the results do not tend to favour one representative group. The following table confirms this nexus:
The reader needs to be aware of the above limitations to qualitative research.

As noted above thirty five executives were interviewed. The questions, which were presented in writing to each interviewee, consisted of the following:

<table>
<thead>
<tr>
<th>Internal Audit / Risk Management Functional Model</th>
<th>Survey 102 Respondents</th>
<th>Interviews 35 Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Combined</td>
<td>30%</td>
<td>35%</td>
</tr>
<tr>
<td>Separated</td>
<td>56%</td>
<td>59%</td>
</tr>
<tr>
<td>Outsourced risk management</td>
<td>2%</td>
<td>0%</td>
</tr>
<tr>
<td>Other</td>
<td>12%</td>
<td>6%</td>
</tr>
<tr>
<td>TOTAL</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

*Figure 4.27  Comparison of survey groupings to interview groupings for S&P/ASX 200 companies*
1. You have a combined board audit and risk committee due to the synergies between audit and risk. Please elaborate on these synergies;

2. You have a separate board risk committee to focus on risks specific to your business. Please elaborate on the importance of these risks;

3. You are having problems with finding enough time at combined board audit and risk committee meetings. How are you dealing with that issue;

4. Do you see any evidence of internal audit and risk management integrating across Australian companies;

5. You have combined internal audit and risk management at the functional level. Can you comment on how this model aligns with the internal audit independence model;

6. You do not have an internal audit function. Can you explain why no such function exists and how you cover assurance requirements for the board and board committees;

7. You do not have a risk management committee. Can you explain how the ASX Principle Number Seven, to recognise and manage risk, is met; and

8. Do you see internal audit as a subset of risk management;

Some of the responses from questions one to three above have been noted in the earlier sections of this chapter. Those responses supported the quantitative findings from the desk-top analysis and survey work. Other responses from questions one to three above are addressed in the last sections of this chapter, where emerging models are discussed.
Questions four and five go to the heart of the governance of risk management in S&P/ASX 200 companies. The extent of integration between internal audit and risk management is a primary objective of this research. In particular these questions help address the extent to which internal audit and risk management are integrating in these leading Australian companies.

4.13.1 Integration of Audit and Risk

All interviewees were asked the question “Do you see any evidence of internal audit and risk management integrating across Australian companies?” The four risk partners with the Big Four companies provided an industry wide focus.

Of the 30 interviewees who responded on this question, 25 (83%) indicated that there is a growing integration between internal audit and risk management. The remaining, 17% stated that internal audit independence concerns were inhibiting integration.

As a result of these discussions a number of themes, or often repeated issues, emerged from the interviews:

1. the synergy between audit and risk;
2. the independence barrier;
3. combined roles;
4. the maturity of the organisation; and
5. the different training, experience and backgrounds for internal auditors and risk managers.

The following sections summarise each of these themes, using comments from the interviews where appropriate.

4.13.2 Synergy Between Audit and Risk

Earlier in this Chapter the survey respondent’s views on the synergy between internal audit and risk management were outlined. That was a strong theme from the interviews.
Firstly, the circular flow diagram (Figure 4.5) was recognised by many interviewees. Management and in particular the risk managers assess the risks to the organisation. These risks are entered into the risk register and become the risk profile. Management then takes those identified risks and designs mitigations to address the risks. The internal auditors then use this risk profile, generated by the risk managers, to design their audit plan for the coming period. The audit plan, prioritised by risk likelihood and consequence, leads to reviews of the action plans, mitigations and internal controls adopted by management. Where these management activities are found to be inadequate or lacking, a new risk arises. An executive from a energy company supported this theme:

When I first started in the governance role I thought that internal audit and risk management must be separated for the traditional independence reasons. Having been in the role for several years, I have softened my view.

When you think of the flow diagram (risk drives the audit plan and outcomes feed back into the risk system) you start to realize it is just one continuous system. (CRO from a CIGS 10 company)

A financial services executive supported this theme:

We see many opportunities for integration with each function leveraging off the other. Good risk assessment allows the audits to focus on the right risks, and conversely, audit findings help establish where the risks are lying. (COSEC from a GICS 40 company)

Synergies were also raised in the context of the number of, and duration of audit committee meetings. It seems that the relationship between internal audit and risk management may be a driver for the form and content of committee meetings. This was observed by an executive from a electricity utility:
At board level a combined committee has recently been reconfirmed. The board see a lot of synergy. Internal audit derive their three year plan from the risk profile. The risks direct work on internal controls. Internal audit uses the risk system to scope out their work, depending on the mitigations. The committee meets six times per annum, four of which have risk management as the number one agenda item. The meetings are now longer to cope with additional risk workload and risk owners now appear before the committee. (CRO – from a GICS 55 company)

The use of the risk register or risk matrix was also seen as a related synergy by a Telecommunications executive. As noted earlier this may be an example of knowledge management at work:

We see strong synergies between risk and audit. At the board level the risk matrix is used to focus attention and direct the internal audit effort. Risks are also raised from internal audit findings, a two way street.

Our risk management group is under the CAE. This group audits management mitigations, provides expert advice on risk, conducts risk workshops and completes the annual risk report to the board. Managers appear before the audit committee to explain their risk mitigation strategies. Two of the six meetings have a strong risk focus. (CRO from a GICS 50 company)

This theme was continued by an executive from a materials company who also saw synergy in the auditors using the risk register as a tool for planning the audit activity:

Yes I do see more integration. In the past internal audit and risk management were separate silos. Now that audit needs to draw its program from the risk managers and also needs to use the risk register tool to allocate audit work, the relationship is becoming much closer. (CRO from a GICS 15 company)
The issue of balancing scarce resources was brought into the equation by an investment company where the audit committee directed resources based on risk and reward trade-offs:

*This company sees strong synergies between internal audit and risk management. Primarily the audit committee is concerned with risk management. Risks are identified and limited resources are allocated to mitigate and control these risks. The role of internal audit is to ensure that the mitigations or controls are in fact in place and are working. The role of the audit committee is to balance risks, mitigations and resources. (CRO from a GICS 40 company)*

The COSO model is used by both internal auditors and risk managers. Auditors use the COSO framework to design audit activities. Risk managers use the COSO risk framework to identify and rate internal controls.

The use of a common model was also seen as a synergy by an industrial company executive who felt that the COSO model facilitated integration between audit and risk, another example of knowledge management:

*The COSO model provides the framework for integration between audit and risk. We look at what is driving a function then determine whether we need a risk response or an audit response. There is also a COSO ERM framework which is used by risk managers and links to the COSO framework used by audit managers. (Company Secretary GICS 20 company)*

Finally, a partner in a Big Four company provided his own view on integration:
Yes, most definitely there is evidence of integration. Many organisations are adopting the three lines of defence model, which brings management, risk and audit into the same cycle. This also includes compliance, fraud, whistle-blowing and ethics. We need to get over the audit looking back and risk looking forward hang-ups from the traditional roles. (Risk Partner - Big Four consultancy)

In Chapter Two, independence was identified as a significant barrier to the integration of internal audit and risk management. Risk management lies at the heart of independence. Agency theory shows us that an independent internal auditor, separated from the agent, can provide the principal with an unbiased view of the integrity of company processes. The next section explores this issue from the interviews with Australian executives.

4.13.3 The Independence Barrier

The audit profession requires that internal auditors must remain independent from management to remain objective. A consumer discretionary executive put this clearly:

I don’t really see evidence of integration, the independence issue will always be a problem. (Company Secretary from a GICS 25 company)

This means that internal auditors cannot fully engage in risk management which is seen as a management responsibility. Arguably, this independence barrier goes further than this and actually prevents internal auditors from rising to top executive positions. If an internal auditor rises to the top executive team and becomes part of management decision making, then that involvement in executive decision making enters a grey area within the audit profession independence and objectivity requirements.
The interviews revealed a number of companies who want audit and risk to remaining separated with integration being “off the table” due to independence concerns. A materials company executive stated this view:

*Risk management is a line management responsibility and internal audit must express assurance over that function and therefore must be independent. Breaching this independence would breach a cornerstone of governance.* (CAE from a GICS 15 company)

An executive from a household retailer supported the independence argument and actually took that one step further. He felt that the independence argument was gaining strength and was leading to the splitting of audit and risk functions, rather than integration. That view was underpinned by signalling theory:

*If you had asked me two years ago if I saw evidence of integration, I would have said yes. However now I actually see things moving the other way. Firms are now getting their ERM firmly in place and they are seeing the benefits. The ASX Principles have been beefed up, but mainly in the area of risk management. This sends a strong message about the focus on risk.*

*My call would be that combined audit and risk committees are now being split up to allow more focus on the two core issues – risk management and the annual accounts.*

*Also the requirement to have internal audit validate the risk management outcomes will keep the auditors in a different camp.* (CRO from a GICS 25 company)

However, arguments on the issue of independence were polarised. While 17% of interviewees supported the upholding of independence, 83% saw integration as the way forward. A financial institution executive saw independence as a historical hang-up, possibly required for less mature companies:
There are purists out there who want to keep internal audit and risk management separate, however it is better to have overlap and cross pollination behind the scenes. (CAE from a GICS 40 company)

This argument was supported by a materials company executive who thought that separation of audit and risk was a legacy from the past. Legacy issues are underpinned by evolution and the impact of the external environment on that evolution. These environmental changes bring a contingency flavour to the integration argument:

*Having internal audit and risk management separated is more historical than due to independence. Internal audit was here first and the role is well understood. Risk management developed out of insurance and looked at different things to internal audit. Since internal audit was already well established, we didn’t want to dilute with risk management. Internal audit focuses on policy and procedures, whereas risk management takes a bigger picture view of commercial strategy and risk matters.* (CFO from a GICS 15 company)

Another executive noted that integration was more likely in smaller companies. That brings up the agency cost argument and whether smaller companies can afford the luxury of employing both a CRO and a CAE. That executive also indicated that within industry sectors, a contingency or environmental perspective might also be behind integration:
Evidence of integration is not obvious, but depends on the size of the company and the industry. If a company is small, a combined risk and audit team, under a multi-skilled manager is more cost effective than two teams. In the financial services industry the CRO is much more powerful and will often have the audit team under the CRO role. In that situation there is a lot of integration. The internal audit profession are a “defensive mob” who are keen to raise the integration barrier. (CRO from a GICS 10 Company)

One executive from a consumer discretionary company also felt that views on independence and integration might differ between industries:

I used to work in a bank where there was no integration due to independence concerns. In my current company, we don’t have an audit function but do everything through risk management. (COSEC from a GICS 25 company)

Another executive indicated that independence and integration can co-exist. If the internal auditors and risk managers are aware of conflicts, they can integrate but use strategies to maintain independence. These strategies were discussed by Christopher et al (2009) in Chapter Two, and include outsourcing the audit of risk areas where the in-house auditors have been involved and ensuring a direct reporting line to the chair of the audit committee:

Can’t see why you separate risk and audit, two sides of the same coin. We would only separate where we want the auditors to validate some risk activity.

We are finding it harder and harder to keep risk and audit issues apart. (CRO from a GICS 20 company)

The next section outlines comments from interview respondents who indicated that risk management and internal audit report to the same executive manager.
4.13.4 Combined Roles

In Chapter Two, under section 2.11 the synergies between internal audit and risk management were discussed. Those synergies were couched in terms of both functions overseeing a management responsibility, both having similar functional objectives and both being systems of internal control.

The same theme emerged from the interviews with a number of interviewees stating that integration had resulted from the shared objectives of risk and audit:

*The areas of internal audit, risk management, compliance, legal and governance are all related. These areas have different skill sets but are all aimed at identifying issues (risks) then resolving those risks by internal control and careful management.* (CRO from a GICS 40 company)

In several cases, the interviewees stated that integration was evidenced by having a single executive presiding over both internal audit and risk management. One risk and assurance executive from a consumer staples company made the following comment:

*Director Group Risk and Assurance looks after risk and the outsourced internal audit function. He reports to the Chief Legal Officer and Company Secretary.* (CAE from a GICS 30 company)

Those interviewed also saw the similarities between risk management and internal audit as working to help integrate risk management into the culture of the organisation. An executive from a Property Trust stated:
Our head of audit and head of risk is the same person. Both risk and audit sit behind the business as a valued advisor, a very mature model, and work towards integrating risk management into the culture. We see the combined model as an efficient, non-silo way to get risk out into the culture. (COSEC from a GICS 40 company)

An industrial company executive advised:

We are at a very early stage with internal audit. Up until recently we had no audit function but each division had a risk champion. The newly formed internal audit both completes audits and advises on risk management. (CAE from a GICS 40 company)

Organisations that combine the internal audit and risk management roles are displaying elements of knowledge management. The auditors and risk managers have different skill sets, but shared objectives and a common outcome: a risk resilient organisation. This aligns with the Grant (1996) concept of production being the coordination of specialists, each who bring different knowledge to a shared problem. Using the common language of risk terminology, statistical method and group problem solving, the auditors and risk professionals both try to drive risk management into the organisation culture. The fact that the auditors and risk managers have both different and common skill sets allows them to better understand each others’ knowledge domain and better work as a team with common goals. The objective of all companies introducing ERM is to embed a risk methodology into the corporate culture. This means that tacit risk management skills need to be converted into an explicit common language understood by all employees. Having the auditors and risk managers working together, using ERM rules, a common risk language, analogy, metaphor and group decision making would better facilitate the sharing of risk knowledge. A competitive organisation wants all employees working together, for the same purpose and with a language that they all understand.
In Chapter Two, the concept of organisational maturity was raised by Caplain (2009) and Richmond (2006). The theme was that in mature organisations the auditors take more of a partnership role with management and the synergies of integrating with risk management may outweigh any independence concerns. The next section outlines those interviewed on the concept of maturity.

4.13.5 Organisational Maturity

The level of maturity of the organisation as a driver for integration was raised by four interviewees. In chapter two, the literature behind life-cycle theory was discussed. Organisations move from a birthing stage, through growth to maturity and then decline. The revenues, competitiveness, management decision styles, bureaucracy and structures change to suit the stage of development. Immature organisations have a culture of blame. Everyone is busy looking over their shoulders to see who is next going to find fault with their work. In such an organisation admitting to errors is a sign of weakness. Senior managers plot to increase their dominance and power. Actions that benefit them personally often over-ride actions that would benefit the company, perhaps an agency theory perspective. Thirty years ago this was a common model for management and there are still some out there today. One executive saw the integration of audit and risk as a way to promote maturity:

Integration is the only way to go. As soon as you make one [audit or risk] bigger / superior to the other, egos take over and outcomes become less optimal. One integrated system allows everyone to grow. Every organisation has a battle with this. Often the CFO and CAE sit in the corporate ivory towers and nobody wants to deal with them as they threaten people’s future. Perhaps, having a de-facto internal audit inside risk breaks the traditional audit policeman / threat / ego issues while effectively still doing the same thing. We don’t have internal auditors, we have continual improvement. (CRO from a GICS 40 company)
In an immature organisation internal audit must remain independent, more of a compliance or policeman like role.

If internal audit gets involved in decision making, the auditors will be blamed when things go awry. In an immature company, competition between executives would prevent an integrated model from taking hold. The CFO would see an emerging CRO as a threat to his long established patch. The relationship between organisational maturity and internal audit independence was captured by one executive from an energy company:

*Maturity is as important as independence. If the organisation sees the internal auditor as a policeman and tries to block or inhibit the auditors, then strong independence with unfettered access is necessary. If the organisation embraces the auditors, gives them open access and sees them as partners working towards a common internal control goal, then the independence requirement becomes much softer.* (CRO from a GICS 10 company)

A mature organisation has a culture where mistakes are seen as a learning experience, people are not blamed for breaches or mistakes and everybody is working towards the common good. In such an organisation a general manager will happily decrease the size of his unit and be rewarded for contributions which may benefit the company but could disadvantage the individual. Agency theory becomes less important as the interests of the principal and agent become more aligned. In such an organisation, the internal auditor, if indeed such a function exists, will contribute to decision-making and be seen as a value adding partner with management. A mature organisation is free from independence barrier issues and can have the risk managers working alongside the auditors. Some Australian companies see themselves as having reached this level of maturity as can be gauged by the comments from a Property Trust executive:
There is a debate going on over whether audit and risk should be separated. We see value in integration. The audit committee uses a risk based approach to audits and audit findings contribute to the risk sets.

This may depend on the culture, if one of blame shifting, may need to have independence. If more mature, risk can work with internal audit with both helping management with their responsibilities”. (COSEC from a GICS 40 company)

It seems that as companies mature, the need for independence lessens and the argument for integration becomes more solid. At the limit, as companies become more mature, could the internal audit profession actually grow into the risk management profession? An executive from the banking sector felt that traditional internal audit was heading for oblivion:

Classical internal audit can no longer exist in a complex and rapidly changing world. In the old world independence was required to maintain the policeman role. Modern mature organisations no longer look at internal audit as policemen / compliance function, but as a valued partner and advisor. The next logical step in this more mature world is for the audit and risk to combine as valued forward looking partners, helping identify opportunities, manage blockers and assist with controls. (A CRO from a GICS 40 company)

Growing levels of organisational maturity might also be a manifestation of knowledge management. An immature organisation is characterised by continued power struggles, excessive control, fear of error or change and a misalignment between the shareholders and management objectives. This is hardly the environment for the sharing of knowledge. Such an environment is not conducive to the conversion of tacit into explicit knowledge. Those with valuable knowledge will not wish to share, as they see power in being the custodians of such knowledge.
A mature organisation, on the other hand, seems to be expressly set up for the sharing of knowledge. Mistakes are used as a learning experience, sharing problematic issues with a wide audience to help prevent similar future problems. The alignment of management and shareholder goals leads to a greater propensity for the distribution of knowledge.

Managers are happy to share their skills as this helps move everybody towards recognised goals. Employees will work with managers to jointly solve problems, thereby converting tacit to explicit knowledge. The risk managers can work closely with the auditors to help facilitate a risk management culture within the organisation.

4.13.6 Prior Development and Experience

Finally a different view, but one aligned with the above arguments, came from an interview with a partner from a Big Four practice. While that interviewee saw evidence of integration, he thought that there was still separation at the intellectual level. That separation may come from the different modes of training, education and experience provided to auditors and risk professionals in the past:

*Risk professionals are educated and skilled in studying the future, applying forecasting and modelling techniques to attempt to frame possible futures and encouraging people to act in light of these predictive theories. Risk professionals use value at risk, price forecasting, risk adjusted return on capital and even jump diffusion to predict the future. Risk professionals can live with ambiguity and are “forward looking” professionals.*
The education received by many in the internal audit profession, principally accounting and finance, has broadly taught these folk to look backwards at what has happened in the past. For audit to integrate with risk the auditors will need to work against some of the natural behaviours from their baseline education and they may need to address blind-spots or areas of discomfort in looking forward and addressing the future environment.

This is not to suggest that auditors are incapable of discussing forecasts and the future, it is more that they show an inclination for embedding themselves in proving the past. The risk people want to get involved in strategy and decision making and the audit people would like to but are not sure how to claim legitimacy in such internal activities and find themselves out positioned in discussions about growth, forecasting and so on. On balance we see few successful functions where the combined interests work well. Where we have seen it work well is usually headed up by a business person with balanced experiences and not one of risk or internal audit. (Risk Management Partner – Big Four)

The above view aligns with the Fraser and Henry (2007) suggestion that internal audit may not have the depth of understanding of risk management that is required to take on the risk management role.

However, as a contrast, some internal audit teams set up the risk systems and conduct training on risk management. In response to question ten in the survey (see Appendix Three) a telecommunications executive noted:
Internal audit is an independent oversight / assurance control. Risk management is a hands-on direct accountability control. The risk management methodology, framework and tools were developed by internal audit, who also provide training and online modules for staff capability development. (CRO from a GICS 50 company)

4.13.7 Alignment of Audit and Risk

The section above provided insight from those interviewed on the levels of integration between internal audit and risk management at executive and functional levels. The final question to the interviewees, “Do you see internal audit as a subset of risk”? is covered below.

This was a rather provocative question, designed to stimulate a range of interesting responses. The author makes no apology for the fact that CROs will see this question in a different light to CAEs.

If the majority of companies see internal audit as a subset of risk management, then that belief makes the integration of internal audit and risk management much more likely. Growing legislative requirements for increased risk management such as ASX Principle Seven, SOX and Turnbull, in an environment where the internal auditors are already on hand, should promote integration. If a company is compelled to appoint an executive over risk management, the CRO may be the logical person to oversee a small in-house or outsourced internal audit team.

Twenty three interviewees responded to this question. Seventeen respondents (or 74%) agreed that internal audit was a subset of the overall risk management framework. Six disagreed and saw risk management and internal audit as distinctly separate functions, driven by internal audit independence. Two of those who disagreed were CAE’s.
4.13.8  Audit as a Subset of Risk Management

Seventy four percent of those interviewed on this question agreed that internal audit is a subset of overall risk management. Those interviewees saw an overarching risk management framework, under which there were a number of components. These components included compliance, internal audit, continual improvement and even late entrants such as sustainability and climate change functions.

Several respondents saw internal audit as a tool of risk management. Risk management was seen as the framework for identifying and mitigating risks, internal audit as a tool for checking on those mitigations:

*We see internal audit as a subset of risk management. Risk management is the main focus and internal audit is a tool under that process used to watch over the health of that risk management.* (CRO from a GICS 40 company)

*Risk management comes first and is all embracing and internal audit is a checking tool that ensures things are on track. Combined units can work and that seems to be happening across Australian corporate life.* (CRO from a GICS 55 company)

*Internal audit is a subset of risk. Risk management determines the big risks and what actions should be mitigating those risks. Once those risks are determined, audit comes along underneath to check on how well the mitigations are being implemented.* (Company Secretary from a GICS 15 company)

One executive from a consumer discretionary company mentioned the “Iceberg” model (as discussed in section 4.11.3, Figure 4.24). In that model, the annual accounts are the tip of an iceberg, the underlying substance being strategy, risk, opportunity management and operational management. In that model, internal audit forms one of the underlying controls that shape the annual accounts:
Yes audit is definitely a subset of risk especially in the holistic iceberg model. In some ways, everything that a company does, every activity, every payment, every opportunity sought, are all subsets of risk management. (Company Secretary GICS 25 company)

A bank executive confirmed that he thought that having internal audit as a subset of risk management helped promote integration between audit and risk:

Yes, internal audit is one facet of the bigger risk management picture. This also helps with the logical move forward and integration. (CRO from a GICS 40 company)

Finally, one executive provided further insight by defining internal audit and risk management as subsets of governance. This overarching governance theme is prominent in the next section, where a small percentage of interviewees thought that internal audit may not be a subset of risk management:

Internal audit and risk management all form part of the governance framework. You can't have one without the other. They are complimentary, but have different skill sets. And yes, internal audit is a subset of risk management. (COSEC from a GICS 20 company)

4.13.9 Audit as Part of the Governance Framework

Twenty six percent of companies interviewed disagreed that internal audit is a sub-set of risk management. Generally these executives felt that internal audit was more a subset of governance than risk management:

No they are both components of governance, but are separate functions requiring separate skills and experience. (CRO from a GICS 25 company)
No internal audit is a subset of the governance framework. They are cousins and closely related. (CAE from a GICS 15 company)

No I asked my internal audit manager, both are valuable parts of overall governance. (COSEC from a GICS 20 company)

The earlier themes of internal audit being backward looking and risk management being forward looking were raised by a financial services executive:

No they are separate. Risk management is forward looking whereas internal audit is backward looking. (CRO from a GICS 40 company)

The independence argument for keeping internal audit and risk management separated was noted by one executive. Independence was used as a reason why internal audit cannot be a subset of, or related to, risk management:

Internal audit cannot be a subset of risk management because internal audit must remain independent. (COSEC from a GICS 25 company)

Finally, it became clear that the answer to the question “Do you see internal audit as a subset of risk management?” depended on the role of the executives interviewed:

It depends on who you talk to. The heads of internal audit would not see it that way, they would argue that internal audit and risk management are equally important – both sides of the same coin. (CAE from a GICS 50 company)

The findings for the above sections, the interviews with thirty five company executives and four Big Four partners can be summarised by the following quotes from three of the Big Four practice partners:
Partner One

There are varying degrees of integration between risk and internal audit across corporate Australia. Many larger, older more traditional organisations still keep audit and risk separated. The banks are making progress with integration, often having audit reporting to the CRO. Where separation is apparent, independence and communication play a role, as does competition between senior executives. Basel II is bringing risk and audit together as operational risk people now do audits on risk mitigation which is expanding the role of both risk and audit. (Risk Management Partner – Big Four)

Partner Two

On integration there is evidence at the oversight (board) level but not so strong at operational level. Risk managers are often a different group of people. The three lines of defence model is starting to take hold, hence more integration. Integration brings the CFO into competition with the CRO and that may pose a threat to the integrated model. Board committees are recognising more and more that risk is more about the risk return trade off. (Risk Management Partner – Big Four)

Partner Three

Internal audit as a subset of RM, does it matter? My personal view is that the two broad activities serve different purposes both directed at securing more consistent and reliable business outcomes. One activity is premised on looking forward and considering the factors most likely and perhaps remotely that will derail the underlying goals and targets of the entity. Where is our value most at risk from both a loss and loss of opportunity perspective? The other is premised on reviewing the actual performances against goals and targets.
The cross-over and interdependency is where the audit program requires risk based skills to unpick or study the exposure in quantitative terms or operational terms in areas outside of finance / conventional educational base. They (risk and audit) are co-dependent in my view. Of course risk based work is performed by the business routinely, it is just not called risk management, it is called doing business. At the same time assurance work and checking and reviewing performance is also done by the business and not called internal audit. (Risk Management Partner – Big Four)

The interviews with executives served to re-confirm and clarify many aspects and issues arising from the desk-top and survey analyses.

These interviews also contributed to the research objectives surrounding the integration of internal audit and risk management.

Eighty three percent of those interviewed agreed that there is a growing integration between internal audit and risk management. The concept of synergy was again raised and the circular flow of the risk and audit processes, the use of the risk register and the combined use of COSO frameworks were confirmed. There may be a KM aspect to that synergy, using the common language of statistics and risk management, overlapping skill sets and group problem solving to turn tacit knowledge into explicit knowledge. The desire by most S&P/ASX 200 companies to foster strong risk management into the company culture, using both risk and audit teams as facilitators confirms this view.

Independence is still a major barrier to audit and risk integration, but by far the majority of those interviewed saw the benefits of integration as outweighing the independence argument. Independence was seen as a legacy issue that is evolving into integration between audit and risk as companies mature. The audit team was thought to be able to maintain independence, once integrated, by using reporting lines to board committees and outsourcing work where conflicts exist.
The majority of those interviewed saw internal audit as a subset of the overarching risk management framework, which has clear implications for organisational structure and governance.

4.14 MODELS FOR MANAGING RISK IN AUSTRALIA

This final section brings the previous aspects of this chapter together. The information gained from the desk-top analysis, the survey and interviews is used to develop four models that S&P/ASX 200 companies are using to structure risk management.

Research objective three required an investigation of the models for risk management that are emerging in the S&P/ASX 200 population. In Chapter Two a model for the governance of risk management was suggested. The model predicted that each leading Australian company would have one of three options for the oversight of risk at board level. Some companies would choose to combine their audit and risk management oversight at board level. Other companies would have a separate board risk committee. And finally, some Australian companies would have no risk committee at the board committee level.

The model for the governance of risk also predicted that at the executive, functional and operational levels, a contingency theme could result in a number of different functional designs. These would range from the strictly separated audit and risk arrangements across the spectrum to fully integrated arrangements. The information gained from the desk-top analysis, the survey and the interviews all support the predictions made at the end of Chapter Two. The models that have emerged from the research to this point are discussed in the next sections.
As part of the interview process, respondents were sent a power-point organisational chart depicting their arrangements at board, executive and functional levels. The organisational charts were drawn from the desk-top analysis, survey responses and where appropriate from publicly available information. This included the annual reports and corporate governance information used for the desk-top analysis. An example of such an organisational chart is included as Appendix Thirteen.

The first question asked at each interview was “how does the organisation chart, which was provided by e-mail, line up with your actual set-up”?

Some minor changes were made to bring these organisational charts into line with the interviewee’s actual organisational arrangements.

The above process resulted in thirty five organisational charts, each validated by the executives interviewed. An example is provided as Appendix Thirteen.

The author then categorised the thirty five organisational charts into four groups, based on the reporting lines, which were discussed in Chapter Two and have been identified in the earlier sections of this chapter:

1. If the audit department reported to a different executive than the risk department, the arrangement was classified as a “Traditional Independence Model”;

2. If both risk and audit reported to a single executive, who was not a professional risk manager, the arrangement was classed as a “Current Merged Model”. The Current Merged Model is overseen by CFOs, CEOs and COSECs, but not CROs;

3. If both risk and audit reported through to a professional risk manager, a CRO, Group Manager Risk or Vice President Risk, the arrangement was classed as an “Emerging Model”; and
4. If a risk management function existed, but no internal audit existed, the arrangement was classed as the “No Internal Audit Model”.

At this point it must again be noted that the thirty five interviewees are not statistically representative of the whole S&P/ASX 200 population. However, Figure 4.27 above shows that the interview classifications are broadly consistent with the survey categories. While not statistically robust, the four classifications extracted from the interviews, and outlined below are reinforced by findings from the desk-top and the survey analyses.

The following Figure 4.28 shows the above four classifications, with the number and percentage of companies falling into each category.

<table>
<thead>
<tr>
<th>#</th>
<th>Risk Governance Classification</th>
<th>Number of Companies</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Traditional Independence Model</td>
<td>7</td>
<td>20%</td>
</tr>
<tr>
<td>2</td>
<td>Current Merged Model</td>
<td>15</td>
<td>43%</td>
</tr>
<tr>
<td>3</td>
<td>Emerging Model</td>
<td>8</td>
<td>23%</td>
</tr>
<tr>
<td>4</td>
<td>No Internal Audit Model</td>
<td>5</td>
<td>14%</td>
</tr>
<tr>
<td></td>
<td>TOTAL</td>
<td>35</td>
<td>100%</td>
</tr>
</tbody>
</table>

*Figure 4.28  Models for oversight of risk management from interviews with S&P/ASX 200 companies*

The next four sections outline the form and characteristics of each of these models. The models are derived from arguments which have previously been discussed in this research:
1. From Chapter Two and the current chapter; the reporting lines identified between risk and audit at the board, executive and functional levels are drawn on as determinants of the models;

2. From the same chapters; the designation of the executive overseeing internal audit and risk management is fundamental to the models;

3. The degree to which independence for the internal auditor is enforced, versus the synergies seen from integration with risk management;

4. The degree to which these functions are involved in strategy and their orientation, be it forward or backward looking; and

5. The maturity of the organisation and existence of an internal audit function.

The final aspect, involves the author’s own views, as an executive manager, having spent over twenty years in professional risk management and internal audit executive positions. Each section outlines comments from interviewees that help support the chosen classifications.

4.14.1 Traditional Independence Model

The traditional independence model is the structure born out of the traditionalist or purist internal audit mould. In this structure the IIA requirement for the internal auditor to be independent and objective dominates. Figure 4.29 outlines a typical structure for this type of model.
The main feature of this model is that internal audit is kept independent from other executive management functions. The risk management team will report to a different executive than the internal audit team. The CAE will report to the audit committee for audit planning purposes and to another executive for performance reviews and budget allocations, often termed “rations”. An executive from an insurance company commented:

*While internal audit and risk management overlap for the 'bigger' purpose of risk management, they must be kept independent of one another so that internal audit can effectively audit the risk mitigations and controls.*

*At our company the internal auditor has a dotted reporting line to the audit committee.*  
*(CFO from a GICS 40 company)*

The CAE may be excluded from the executive decision-making team for independence reasons. Being part of the decision-making team goes against the underlying philosophy of independence and objectivity. Therefore, in such a model the CAE is often relegated to a third line management position of lower influence.
The CAE may try and use the direct reporting relationship with the board audit and risk committee to maintain some authority. A COSEC from a television network reflected:

*We ensure that the internal audit function is kept separate from risk management so that internal audit can review the ERM system from an objective point of view. Also risk management is about day to day operations and an involvement in such activities. We try to keep internal audit away from day to day stuff which is management’s responsibility.* (COSEC from a GICS 25 company)

The risk management function, reporting to a different executive, who may be head of strategy, is a forward looking function that deals with the risks that stand in the way of achieving future objectives. The risk management team flesh the risks out of future strategy, ensure mitigations are in place and report on the progress of those mitigations to the board audit and risk committee. The separate internal audit function is more of a backward looking compliance role. The internal auditors review management controls, retrospectively, and report deficiencies to the board audit and risk committee.

In the traditional independence model, there may be tension between management and the auditors. Management see the auditors as policemen, working behind their backs to report negative issues through to the board committees.

This arguably shows a lack of maturity in these organisations where management is fearful of negative audit comments, rather than working as a team to embrace suggestions for improvement.

Clearly, in this model the auditors follow the IIA prohibition and do not engage in risk identification, assessment, evaluation or mitigation. They restrict their work to using a risk based approach to planning and will usually check on mitigations as part of the compliance role. A consumer discretionary company executive outlined the following agency theory flavour:
The risk managers identify risk and determine the inherent and residual risk. The internal audit needs to keep independent to validate the residual risk and give both management and directors confidence that enough is being done to spot and manage risks. (CFO from a GICS 25 company)

However, not all companies in the Traditional Independence Model see a strict separation between audit and risk. A electricity network executive noted:

*Internal audit is kept separate but [with] lots of communication and cross-over. The head of internal audit reports to the audit committee and functionally to the CEO. The audit and risk areas collaborate on the use of the risk register, fraud control, training sessions and bounce ideas off one another.* (CFO from a GICS 55 company)

The next model identified from the organisational charts brings internal audit and risk management closer together.

### 4.14.2 Current Merged Model

In this model risk management and internal audit both report through to a single executive, who is *not* a risk professional. This is the most common arrangement in the S&P/ASX 200 companies.

The executive presiding over both risk and audit is usually a CFO, CEO or COSEC. The CAE may still report through to the audit committee as a concession to the IIA’s independence requirements.

However, in reality a powerful CFO or similar executive will wield all the influence. In such a model the CAE is again relegated to a third line management position of lower influence, but will try and use the direct reporting relationship with the board audit and risk committee to maintain authority. An insurance company executive noted:
Our internal auditor reports through to the same executive as our risk manager. To maintain independence, our internal audit has a dotted line through to the chair of the audit committee. (CFO from a GICS 40 company)

The following figure gives a general indication of such a model.

Figure 4.30  Current merged model

In the author’s view we are likely to see more integration between risk and audit in this model. The CFO will move resources around to align with the tasks at hand, perhaps without a lot of concern for audit independence.

With the CFO as head of strategy presiding over both risk management and internal audit both these functions may be more forward looking functions. The risk and audit teams may work more closely together.

The risk management team identifies risks to future strategy and works with audit to ensure mitigations are in place and to report on the progress of those mitigations to the board audit and risk committee.
The internal auditors, more closely linked to risk will use the strategic risks to map out a program going forward and work with management to review actions that address risk. One energy company reported:

*We used to have an outsourced internal audit function. The firm that filled that role saw much greater integration between audit and risk than the independence traditionalists who see risk management as forward looking and audit as backward looking.* (COSEC from a GICS 40 company)

There will still be tension between management and the auditors but since the auditors mix and contribute to management decisions, through the risk team, they are less likely to be viewed as policemen and more as a value adding part of management. Organisations that adopt such a model may be more mature, as suggested by the interviewees, than those with the traditional model above. The work of audit and risk is embraced by management as contributing to the greater company good and suggestions are welcomed rather than seen as criticism. A food processing executive commented:

*Internal audit is viewed as an independent function, but closely integrated with risk management groups and is responsible for assessing the risk process and framework.* (CFO from a GICS 30 company)

In this model the auditors may engage in risk identification, assessment and evaluation but perhaps not mitigation. Indeed members of the risk and audit teams will exchange roles for development purposes. A beverage manufacturer noted:

*The assurance program includes a Control Self Assessment (CSA) program, which is a questionnaire requiring managers of key processes and functions in the Company to advise on the effectiveness of the controls that are in place to minimise risks in the business.*
Action plans must be developed to improve the control, where the control is related to a risk considered significant under our ERM program. The assurance function also includes internal audit, which focuses on the specific risks in the business as agreed with executive management and also reviews the response on the CSA on a random basis to ensure that responses provided by management are correct. (Executive from a GICS 30 company)

The next section summarises the third model developed from the organisational charts provided in the interviews with thirty five company executives.

4.14.3 Emerging Model

In this model, the CRO has reached the executive team and is part of the executive decision making for the organisation. In the emerging model, many of the risk functions that traditionally reported through to the CFO have been transferred across to the CRO, or a similarly named risk professional. An industrial company executive advised:

The title is Group Risk Manager, responsible for risk management and internal audit. (CRO from a GICS 20 company)

The following figure portrays the type of arrangement seen with the emerging model.
In section 4.13.8 above, we discussed internal audit as being a sub-set of risk management. In the emerging model internal audit is seen as a sub-set of risk. Internal audit is totally integrated into the risk management culture and synergy with risk is seen as more important than independence. The CRO will move resources around to ensure that the right experience is aligned with the risk problem being addressed. This is another example of a knowledge management approach. A materials company executive commented:

Absolutely – I see evidence of integration. The internal audit program is driven by the risks to the business. We have recently appointed a CRO, and part of his job will be to manage the outsourced internal audit function, directing them to the biggest risks. Internal audit respond to risk and are driven by risk. (COSEC from a GICS 15 company)

The CRO will be deeply involved in strategy, ensuring all the functions that he oversees are forward looking functions. The risk and audit teams will work closely together and eventually may combine, losing the traditional internal audit connotation. The auditors will still review risk mitigations but so will members of the risk team. A telecommunications company executive said:
The merging of risk and audit under a single executive has become the industry standard. The roles being advertised that now head up audit and risk are called Director of Risk, Group Manager Assurance, or Director Risk and Audit. (CRO from a GICS 50 company)

There will be little tension between management and the auditors as the risk team are viewed as a value adding part of management. Using the interviewee’s terminology the organisation is mature and decisions made for the benefit of the company are valued over decisions that benefit one individual executive. The work of the risk team, including internal audit, is embraced by management as contributing to the greater company good and suggestions are welcomed rather than seen as criticism.

In this model there are very few limitations to what the auditors can undertake in the risk world. The independence and objectivity rules are weighed against the benefits of integration. The internal auditor may still have a direct reporting line to the audit committee, to address any independence issues.

A retail company executive stated:

*Internal audit is managed through the risk management group with a reporting line to the CEO, the CFO and the chair of the audit committee.* (CFO from a GICS 30 company)

The growing integration between internal audit and risk management might promote a greater use of outsourced internal audit. As integration grows, there will be more areas present where the in-house internal auditors cannot conduct audits because they have been involved in development in those areas. Using outsourced resources would overcome these independence problems.
4.14.4 No Internal Audit Model

Five of the executives interviewed, confirmed in their organisational charts, that they had no internal audit function. These companies comprised 14% of the thirty five interviewed. The interesting question that arises is whether these companies are just the smaller, GICS 15, materials start-up companies or is there a new paradigm emerging. A new model where risk management has become the leading light and where the traditional internal audit has faded into the shadows?

In section 4.12 above, companies were interviewed that had no formal internal audit function, but had risk management, compliance or continual improvement functions as de-facto auditors. These companies stated that they had outgrown the internal audit classification with its independence barriers, its backward looking compliance approach and with a management view that internal audit adds little value.

Figure 4.32 below summarises the no internal audit model arrangement.

Figure 4.32 No internal audit model
One of the companies grouped into this model was small, having revenues of only $223 million. This might support the agency theory suggestion that this model includes only smaller, immature companies. A small mining company executive commented:

*We have no internal audit function. If the board wants an issue investigated, we ask KPMG. This has recently been about large contracts.*  (CFO from a GICS 15 company)

However, the interview comments from two other companies suggested that they had excluded internal audit from their organisational structure on purpose. A Property Trust executive stated:

*Our company is a Managed Investment Scheme (MIS) with an AFSL licence. As such the regulators require a very strong compliance system. The Compliance Manager has a program of work that checks on internal controls (similar to internal audit). The company also has external reviews over compliance done by KPMG.*  (COSEC from a GICS 40 company)

Another Property Trust executive stated:

*I complete the risk reviews for the organisation and keep abreast of internal controls. When I find a problem or issue, or a mitigation is required, I allocate the solving of that problem to either internal team members or external experts.*  (CRO from a GICS 40 company)

This CRO has implicitly taken on an internal audit role.

The remaining two companies in the No Internal Audit Model have larger revenues, an average of $1,412 million, and a familiar theme is continued. A retail executive explained:
No internal audit is the minority but is not unusual. We have strong centralised shared services and other functions such as treasury, therefore we don’t need a team of auditors running around the country side. We have a peer review and continual improvement model that in part is like internal audit - we pull in experts when necessary. Because we don’t have internal audit, the external auditors do a little more work and we often ask them to dig deeper on some issues. If we had an internal audit we would not call it that, because of the negative connotations - it would be called risk management. (COSEC from a GICS 25 company)

A television network executive commented:

Firstly, our parent is under SOX, hence we have to feed into that requirement. Secondly, through our risk management function, we pull PWC in to do fraud control, IT system evaluations and problem areas that come up in the risk work, a de-facto internal audit. Also our external auditors do a lot more work on the control environment, partly due to SOX, partly because we don’t have an internal audit, and partly because we ask them to. (CFO from a GICS 25 company)

The no internal audit model is about as distant from the traditional independence model as a company can get. The no internal audit model is out on the future margin where perhaps independence has been over-ridden by the mature outlook of the company. This model relies on the synergy between risk management and control reviews and where the CRO is working with the synergy between a number of risk related functions.

This model is forward looking and having functions such as risk management and continual improvement under the risk management wing, forces that direction.
On a continuum, commencing with less maturity across to greater maturity, this model may lean towards the more mature end. The functions are there to assist management to grow rather than confronting management with their deficiencies. This again is an example of knowledge management at work.

In summary, the final section of this chapter develops four broad models for the governance of risk management within leading Australian companies.

These models are based on:

1. the reporting lines for internal audit and risk management;
2. the designation of the executive overseeing internal audit and risk management;
3. the existence of an internal audit function;
4. the degree to which independence for the internal auditor is enforced, versus the synergies seen from integration with risk management;
5. the degree to which these functions are involved in strategy and whether such functions are forward or backward looking; and
6. the maturity of the organisation.

The fact that four broad models for audit and risk management have been identified may reflect the newness of the risk management discipline. DiMaggio and Powell noted that organisations start out with very diverse structures, which eventually become more homogenous over time. In Australia we may be going through the “shake-up” period where coercive, mimetic and normative isomorphism is shaping the future for risk management arrangements.
Research objective three sought to establish a number of models for the governance of risk management in the S&P/ASX 200 companies. The above models identified facilitate the meeting of that research objective.

The next chapter, the conclusion, summarises the above findings, discusses the value of each finding and suggests avenues for further research.
CHAPTER FIVE - CONCLUSION

5.1 INTRODUCTION

In this chapter the findings from the research are summarised. The findings are placed into context with the theories outlined in Chapter Two (see Appendix Twenty One) and the value of each finding is discussed. Possible future research is also proposed.

The primary research aim was to examine the organisational structure that is used to facilitate risk management in leading Australian companies, including an analysis of the tensions and strengths of integrating risk management with internal audit.

The methodology involved a desk-top analysis, a survey and qualitative interviews with a sample of executives from the S&P/ASX 200.

5.2 COMBINED BOARD AUDIT AND RISK COMMITTEES

One of the objectives of this research was to investigate the structure of risk management at the board committee level. This objective included the reasons for having board audit committee oversight of risk management.

Institutional theory indicated that companies will tend to follow the practices adopted by companies considered leaders in their field. Such imitation can be underpinned by powerful stakeholders, the desire to seek legitimacy or even pressure exerted by respected peers such as educational institutions and industry associations.

Institutional theory explains why 73% of S&P/ASX 200 companies govern risk management through the board audit committee. The Australian situation closely follows the overseas experience where the board audit committee is the top level of risk management governance. This conclusion supports prior research completed by KPMG (2005) and Subramaniam et al (2009).
Figure 5.1 Board risk committee arrangements in the S&P/ASX 200 companies

The main reason given by respondents for using the board audit committee to oversee risk management was the synergy between audit and risk.

Figure 5.2 Reasons for combining board audit and risk committees

The respondents and interviewees discussed the “circular flow” between audit and risk. The internal audit program is determined by the risks that a company faces. The internal audit work then uncovers more risks which are added to the risk portfolio.
There is a natural flow of synergy. The outcomes of strategic and operational risk management drive the internal audit plans. The outcome of the internal audit work finds more risks and tells us how we are going on risk management, both of which feed back into risk management. (COSEC from a GICS 10 company)

Interviewees felt quite strongly that a combined board audit and risk committee facilitated the synergy between audit and risk. Having risk, control issues and the annual accounts dealt with in the same forum was seen as optimal.

As a board we realised that we could not separate risk from audit and do our job. How can you account for assets and set up reserves without assessing risk? (Connelly, 2009)

The emerging “three lines of defence” model, being adopted by some financial services companies was also cited as a synergy between audit and risk. The fact that the annual accounts are the score card for the companies risk management activities was also seen as a synergy.

Audit is all about the annual accounts and the balance sheet but these are just the outcome of all underlying opportunities, threats and how risks are dealt with. The accounts are just the “tip of the iceberg”. (CRO from a GICS 25 company)

Again, those executives interviewed saw a combined board audit and risk committee as the best way to manage these synergies. Having risks assessed and mitigated through one committee, with a separate committee reviewing the annual accounts was cited as a sub-optimal outcome. These findings extend the work by Subramaniam et al (2009) by outlining the reasons that boards chose to govern risk through the board audit committee.
The synergy between internal audit and risk management is an example of knowledge management (KM). The relationship between risk management and internal audit exhibits all of the characteristics cited by KM proponents. Power theory may also play a role in this synergy.

Internal audit and risk management use similar risk identification processes, have a common risk management and statistical language and use group problem solving to determine outcomes. They have overlapping knowledge domains and both work towards the conversion of tacit risk mathematics into explicit language that helps embed risk management into the culture.

The oversight of risk management through the board audit committee is the preferred mechanism. Utilising the synergies between internal audit and risk management, this structure overcomes many of the problems with alternative structures.

A combined board audit and risk committee is the better practice and will eventually displace separate board risk committees. Having risk, audit and the annual accounts reviewed in the one venue is a persuasive argument. The synergies between audit, risk and the annual accounts, through KM promote a sharing of information between departments and across the corporate culture.

The synergies between audit and risk are a main theme in this study and are a key driver for the better practice models developed. Further definition and investigation of such synergies could be a separate and all inclusive research project.

Such a project could look into the conflict between the benefits of knowledge management and the audit profession requirement for independence.
5.3 SEPARATE BOARD RISK COMMITTEES

A minority of the S&P/ASX 200 companies govern risk management through a separate board risk committee. This alternate model has been adopted by 17% of companies. Problems were identified with this model by both survey respondents and those interviewed. This arrangement was stronger in the financial services and the consumer products sectors.

Contingency theory suggested that environmental factors will determine the governance structures that a company adopts.

Financial services companies are faced with a unique environment where their core business is the management of risk. The financial services sector uses the board risk committee arrangement to manage credit, market, trading, liquidity, capital adequacy, regulatory and compliance risk. The fact that many separate board risk committees evolved from former credit and loan mandate committees supports this environmental perspective. Signalling theory might also play a role given the high profile bank failures over recent years. Banks now want to signal to the market that they have sound risk management practices.

*In the global investment banks the CRO is very powerful. He would have legal, tax, compliance, operational risk and audit reporting through to him and would have the power to veto transactions. In Australia this model exists but is only starting to take hold.* (COSEC from a GICS 40 company)

According to interviewees, signalling theory underpins the use of board risk committees in the consumer products sector.

Those interviewed confirmed that these companies set up separate board risk committees to manage high profile industry risks such as food hygiene or telecommunications infrastructure risk. Given their visibility, these companies want to signal a commitment to risk management.
The study has shown that, a separate board risk committee is not the ideal practice. The majority of financial institutions surveyed still have the board audit committee overseeing risk management. The separate board risk committee structure inhibits the synergies between audit and risk. Having evolved from former credit committees, these separate risk committees are dominated by management. Good practice governance requires that board committees are composed of non-executive directors, with management attendance by invitation only. The link to earlier credit committees also means these committees tend to focus on financial risk rather than holistic ERM.

In the companies with separate board risk committees, boundary disputes occur with the audit committee. The author has had first-hand experience with this problem and feels it would be useful to further explore and define this negative issue.

Interviews confirmed that companies with a separate board risk committee had demarcation issues with the board audit committee.

In regard to synergies, I see the flip side as more important. Because risk and audit are so closely aligned and overlap, having separate board committees would cause unnecessary complications. The board committees would be continually competing over jurisdiction and what falls into what committees’ area of expertise. (COSEC from a GICS 15 company)

To the author’s knowledge, this is the first work, both within and outside Australia that attempts to explain the motives behind forming board risk committees.

5.4 NO BOARD RISK COMMITTEE

The investigation explored S&P / ASX companies that indicated they do not have a board committee responsible for risk management.

The study found that 10% of S&P/ASX 200 companies have no board risk committee.
The executives controlling these companies claimed that either the full board or an executive committee administered risk management.  

*The chairman is not keen on merging audit and risk as he wants the full board present when significant risk issues are being discussed.* (CAE from a GICS 10 company)

Many of these companies are small, often being mining start-up companies, still in the development phase of their operations. Life cycle theory would posit that these companies are in the birth or early growth stage where management and governance structures are less well developed.

*Our company is a young company and the board are just getting on top of risk management. The risk management function is evolving, soon to be formally implemented.* (CFO from a GICS 15 company)

Others are subsidiaries of larger corporations and may rely on the risk management services provided by the parent.

There has been no prior research on companies that have no board risk committee therefore this finding contributes to our understanding of board governance.

### 5.5 SKILL, TIMING AND WORKLOAD ISSUES

Given the move for boards to add risk management to the activities of the board audit committee, a research objective relating to skill, timing and committee workload issues was justified.

Two issues related to the governance of risk management emerged from the overseas literature.

Cohen et al (2002) contended that, with the increasing importance of risk management, boards are having difficulty finding directors who have both financial and risk management skills.
Fraser and Henry (2007) suggest that with the integration of audit and risk management, board committees are struggling to find enough time to deal with both financial and risk management matters.

This research indicates a different story in Australia which contradicts Fraser and Henry (2007), Zaman (2001) and Spira and Page (2002). In general, the S&P/ASX 200 Australian companies are not experiencing the difficulty noted in the overseas literature with finding skilled directors and finding sufficient time at committee meetings to deal with both financial and risk matters.

Comments from survey respondents and the interview responses revealed that it is common for a board audit committee to devote a number of committee meetings to risk management issues and the remainder to financial and audit issues. The general thrust was to set a risk agenda for committee meetings around the strategy formation period, September to March.

The remaining meetings, April to August, focused on audit, financial matters and the annual accounts.

\textit{The meetings around financial year end are predominantly about finance and accounting matters. The meeting around strategy time is largely about risk. (COSEC from a GICS 20 company)}

Four audit committee meetings per annum appeared common and several respondents commented that they had moved to six meetings per annum to deal with the additional risk workload.

\textbf{5.6 ENTERPRISE RISK MANAGEMENT}

The survey work sought to establish the status of ERM implementation across the S&P/ASX 200 companies. This status was required to explore any relationships between ERM implementation and risk management structure.
This type of maturity evaluation has been completed overseas (Beasley et al, 2005, Kleffner et al, 2003, Colquitt et al, 1999 and Miccolis et al, 2001) but to the author’s knowledge, no such metric has been attempted in Australia.

![Graph showing adoption of ERM by S&P/ASX 200 companies]

**Figure 5.3 Adoption of ERM by S&P/ASX 200 companies**

Australian companies self reported sound awareness of ERM and the majority are well progressed with ERM adoption. The larger companies seem to be more advanced with their ERM maturity.

This supports the agency theory link between company size and the existence of risk management committees found by Subramaniam et al (2009). This could also be explained by life-cycle theory as these companies are in the mature segment of their existence, where governance arrangements become more complex and structured. There is no particular industry segment that is ahead of others on ERM implementation.

This is the first time that Australian companies have been assessed for ERM implementation status. These results can now be compared with the overseas experience. It is also clear that ERM is important to leading Australian companies.

With the majority having either a partial or a full framework in place, the option to ignore ERM would be difficult to accept.
The small percentage of companies that are either ERM unaware or still investigating ERM may not earn any credits from rating agencies or institutional shareholders.

This finding means that all leading Australian companies will eventually need to consider their risk structure. As well as ERM implementation, companies need to consider the board committee arrangements, executive oversight and relationship between internal audit and risk management.

Additional, more detailed, research could be conducted on the level of maturity of risk management in leading Australian companies. The literature indicated that the maturity of risk management can be measured by:

1. The absence of silos, with an integrated holistic approach;
2. Commencing risk management in the strategic process;
3. Using a portfolio approach;
4. The use of blended products;
5. Embedding ERM in the day to day processes of the company; and
6. A strong “tone at the top”, or board and management commitment to ERM.

A future research project identifying company progress on each of the above variables would be useful in the Australian context.

5.7 EXECUTIVE OVERSIGHT FOR RISK MANAGEMENT

One of the gaps in the literature, noted in Chapter Two, was the lack of research in Australia regarding executive oversight of risk management.

Overseas research such as Tillinghast (2001) shows the CFO had taken the lead role in financial and risk matters. Canadian research such as Liebenberg and Hoyt (2003) and Kleffner et al (2003) has indicated that the CRO is now taking a lead role in risk management in a growing number of companies.
In the S&P/ASX 200 companies the CFO is the lead executive responsible for risk management with 32% of companies having risk reporting to the CFO. Institutional theory may be behind this finding with companies imitating leading international practices to gain legitimacy.

The CRO is however, close behind the CFO, with twenty six percent of companies using the CRO to oversee risk matters. In the energy, telecommunication and financial sector, the CRO has replaced the CFO as the senior executive overseeing risk management. The unique environment facing the finance and energy industry, including the requirement to manage complex derivatives might be driving the appointment of these powerful CROs.

To the author’s knowledge, there has been no prior study on the executive oversight of risk management in Australia. These findings will help organisations decide whether they need to appoint a CRO or can use the existing CFO in the risk management role.

"Integration brings the CFO into competition with the CRO and that may pose a threat to the integrated model. (Risk Management Partner – Big Four)"

The CFO is being challenged for the top risk management role by the CRO. Ten years ago the CRO was unknown. Now with regulatory pressure for ERM, and a focus on signalling to regulators, the CRO will eventually overtake the CFO as the pre-eminent risk professional.

An option for future research is the divergent roles for CROs. Is a CRO in one industry the same as a CRO in another industry? Do the CROs in different industries have completely different backgrounds, skills and even different job descriptions?
5.8 INTEGRATION AT THE FUNCTIONAL LEVEL

One of the prime objectives of the research was to ascertain the level of integration between internal audit and risk management in leading Australian companies.

Respondents to the survey reported that thirty percent of S&P/ASX 200 companies had combined risk management and internal audit at the operational level.

This finding aligns with international experience (Walker et al, 2002 and McNamee and Selim, 1998) where audit and risk are moving closer together.

The two main reasons given for this integration were the synergies between internal audit and risk management and the fact that both are internal controls. Both functions are seen as control mechanisms within the governance framework.

The combined internal audit and risk management units stated that they had no concerns with independence. These functional units used outsourcing, Chinese Walls and reporting lines to the chair of the audit committee to overcome independence problems.

Fifty six percent of survey respondents stated that internal audit and risk management are separated at the functional level, primarily due to independence concerns. However, the interviews with senior executives indicated that at least half of this fifty six percent had both internal audit and risk management reporting to a single executive.

*The merging of risk management and internal audit under a single executive has become the industry standard. The roles being advertised at the top level are now called Director of Risk or Chief Risk Officer. (CRO from a GICS 50 company)*

According to those interviewed, such an arrangement displays a higher level of integration than if the two functions reported to different executives. Eighty three percent of those interviewed saw a growing integration between internal audit and risk management.
The rationale for having internal audit and risk management separated is nonsense. In most cases the separated internal audit and risk management both report to the CFO, thereby destroying any independence. (COSEC from a GICS 25 company)

The maturity of the organisation, as defined by interviewees, emerged from the interviews as a strong driver for integration between internal audit and risk management.

Interviewees noted that immature organisations required strong independence to administer a strict compliance role for the auditors.

Maturity is as important as independence. If the organisation sees the internal auditor as a policeman and tries to block or inhibit the auditors, then strong independence with unfettered access is necessary. If the organisation embraces the auditors, gives them open access and sees them as partners working towards a common internal control goal, then the independence requirement becomes much softer. (CRO from a GICS 10 company)

Mature organisations saw auditors as partners, working towards a common internal control goal. In mature organisations, the benefits of synergy and integration over-ride the need for independence. There is scope for further research on the definition of maturity and the role such maturity plays in the links between internal audit and risk management.

Seventy four percent of interviewees saw internal audit as a subset of risk management. This fact in itself must lead to greater coordination and integration, as internal audit seeks to find a place in the risk management framework.

However, it appears that, in the S&P/ASX 200, at least thirty percent, and up to sixty percent, favour the practicalities of integration over independence.
The author has no doubts that internal audit will continue to integrate with risk management. Classical internal audit can no longer thrive in a world where risk management has become the prime regulatory and corporate focus.

*Classical internal audit can no longer exist in a complex and rapidly changing world. In the old world independence was required to maintain the policeman role. Modern mature organisations no longer look at internal audit as policemen / compliance function, but as a valued partner and advisor.*

*The next logical step in this more mature world is for the audit and risk to combine as valued forward looking partners, helping identify opportunities, manage blockers and assist with controls.*

*(A CRO from a GICS 40 company)*

The author is hopeful that this work will encourage others to study and write on this integration, investigating whether the audit profession needs to embrace some very significant change.

### 5.9 OUTSOURCING OF INTERNAL AUDIT

One of the research objectives was to investigate how the outsourcing of internal audit impacted on the governance over risk management.

This study found that eighty two percent of S&P/ASX 200 companies have an internal audit function. It is clear that leading Australian companies now consider having an internal audit function as important.

This study also found that approximately thirty percent of leading Australian companies outsource their internal audit function. This is broadly consistent with previous studies.

These are interesting findings in light of the integration between internal audit and risk management. Companies that have outsourced internal audit can have the auditors reporting through to a risk management executive.
This opens a path to greater integration, rolling the internal audit into the risk group and branding the activities under the corporate governance or risk management banners. This finding confirms and updates previous studies. The high incidence of internal audit functions in the S&P/ASX 200 companies suggests that other Australian companies may, in the future, follow suit.

Eighteen percent of S&P/ASX 200 companies have no internal audit function. Interviews revealed that these companies were comfortable without an internal audit presence because the ASX Principles do not mandate an internal audit function. These companies conducted internal audit activities in other guises, such as through the risk management, compliance or continual improvement functions. This finding is important to the IIA and audit profession. Those bodies have been lobbying for mandatory internal audit under the ASX Principles and under company law.

5.10 MODELS FOR MANAGING RISK

One of the research objectives for this study was to search for identifiable models for risk management in the S&P/ASX 200. This section looks at the models that were extracted from the surveys and interviews with risk executives.

The research categorised thirty five organisational charts, provided by interviewees, into four groups:

**Model One  Traditional Independence Model**

In this structure, the requirement for the internal auditor to be independent and objective dominates. The risk management team will report to a different executive than the internal audit team.

The risk management function is more likely to be involved in strategy. The internal audit function is more likely to be a compliance role. Interviewees felt that this model suited less mature organisations.
Model Two  Current Merged Model

In this model risk management and internal audit both report through to a single, non risk professional, executive. There is more likely to be some integration between risk and audit. With the CFO as head of strategy presiding over both risk and audit, these functions may be more forward looking functions. Since the auditors mix with and contribute to management decisions they are more likely to be viewed as a value adding part of management. Interviewees felt that organisations that adopt such a model are beginning to show the maturity to overcome the independence barriers.

Model Three  Emerging Model

In this model, the CRO has reached the executive team and is part of the executive decision making for the organisation. In the emerging model, many of the risk functions that traditionally reported through to the CFO have been transferred across to the CRO. Internal audit is totally integrated into the risk management culture and synergy is seen as more important than independence. Interviewees felt that this model is gaining popularity. The organisation is mature and decisions are made for the benefit of the company. The work of the risk team, including audit, is embraced by management as contributing to the greater company good and suggestions for improvement are welcomed rather than seen as criticism.

Model Four  No Internal Audit Model

A number of companies had no formal internal audit function but had risk management, compliance or continual improvement functions as de-facto auditors. The no internal audit model is probably a futuristic extension of the emerging model.

Having functions such as risk management and continual improvement under the CROs wing forces a forward looking direction.
This is a more mature model where risk and de-facto audit functions exist to assist management, without some of the tensions noted in the more traditional models.

In the author’s view the emerging and no internal audit model will eventually replace the two more traditional models. As governance matures, with a focus on risk management the prominence of the CRO will grow and the need for compliance auditing will lessen. A strong risk group will partner with management on strategic risks and audit like reviews will be carried out by risk managers or de-facto auditors from risk, compliance or business improvement functions.

Having identified the models from interviews, it would be useful to conduct a study to find out the exact statistical proportion for each model in the wider Australian corporate population. It would also be helpful to establish whether any trends are apparent in respect to these models, perhaps with a longitudinal study.

Company maturity and the relationship to both the internal audit and risk management models could be investigated. The study found, from interviews, that mature organisations do not require internal audit to be strictly independent.

5.11 LIMITATIONS OF THE RESEARCH

The research has two known limitations, both of which were discussed extensively in the relevant chapters:

1. The interviews with company executives may not be representative of the full population of the S&P/ASX 200 companies; and

2. The percentage of companies which partially combine internal audit and risk management functions was difficult to determine, and some assumptions were required.
Interviews with Executives

The survey achieved a 59% response rate. That means that 102 valid responses were received from 173 S&P/ASX 200 companies. The interviews, on the other hand were only conducted with 35 respondents, those that had agreed to interviews from the above surveys.

One of the primary concerns with the interviewing method is sampling, that is, validity and reliability may be compromised in small scale interviews that cannot be generalised to the wider population. In this research, no attempt is made to generalise the results of the interviews to the full S&P/ASX 200 population. Rather, the interviews provide a rich source of information that supports and elaborates on findings from the desk-top and survey results.

Internal Audit and Risk Management Reporting to the same Executive

Fifty six percent of respondents to the survey indicated that they had a separate risk function to the internal audit function. This appeared high in the author’s practical experience. The problem uncovered was that many of these respondents had reported a separated function, when in fact the internal audit and risk management functions reported to the same executive.

To investigate this dilemma further, the interviews with company executives were examined. Thirty five interviewees provided organisational charts that outlined the reporting structure for internal audit and risk management within their organisation. Again it should be emphasised that the interviews cannot be fully representative of the full S&P/ASX 200 population due to the small number of interviews.

The following table compares the responses from the one hundred and two survey responses to the thirty five responses from the interviews. The interview sub-set is consistent with the survey percentages:
Figure 5.4  Comparison of survey responses to interview responses in the S&P/ASX 200 companies

In the interviews 20 respondents stated that their internal audit and risk management functions were separated. That is the 59% outlined above. From that group of twenty interviewees, thirteen, or more than half, reported that their internal audit and risk management reported to a single executive.

Therefore, using a conservative assumption, up to half of those companies in the survey which reported separated audit and risk functions may have internal audit and risk management reporting to the same executive.

5.12  CONTRIBUTIONS FROM THE RESEARCH

In this section the value of each finding, both for academic literature and for professional practice, is discussed. The final section also outlines the twelve articles that have been written from the thesis, nine of which have already been published.

Combined Board Audit and Risk Committees

Seventy three percent of S&P/ASX 200 companies oversee risk management through the board audit committee.

<table>
<thead>
<tr>
<th>Internal Audit / Risk Management Functional Model Comparison of Survey to Interviews</th>
<th>Survey 102 Respondents</th>
<th>Interviews 35 Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Combined</td>
<td>30%</td>
<td>35%</td>
</tr>
<tr>
<td>Separated</td>
<td>56%</td>
<td>59%</td>
</tr>
<tr>
<td>Outsourced RM</td>
<td>2%</td>
<td>0%</td>
</tr>
<tr>
<td>Other (includes no risk or audit)</td>
<td>12%</td>
<td>6%</td>
</tr>
<tr>
<td>TOTAL</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>
This finding supports the work by KPMG (2005) and Subramaniam et al (2009) both of whom had similar findings. The finding extends both of these prior works by explaining why the majority of leading companies chose the audit committee as the preferred governance mechanism.

The synergy between internal audit and risk management was cited by those surveyed and interviewed as the main driver behind using the audit committee as the oversight body for risk management. This was suggested to be linked to knowledge management (KM).

The concept of synergy between internal audit and risk management is new to the literature and opens future possibilities related to KM and the evolution and maturity of companies.

There is not much literature on knowledge management in Australia and explicit knowledge management seems to be underused by Australian companies, Guthrie (2001). Therefore opportunities exist to explore this further with respect to corporate governance. The implication is that management should be more explicitly considering knowledge management as a tool for corporate governance improvement as it will result in competitive advantage.

When the link between synergy and KM is applied to other similar or overlapping functions, for example, sustainability and continual improvement, there are competitive advantages to be gained by the business.

Practically, having a combined board audit and risk committee in the majority of leading Australian companies is an important finding for all Australian companies. Adopting such a model would align the company with both S&P/ASX 200 and international leaders and allow the company to benefit from the synergies between internal audit and risk management.

This finding is particularly practical for those companies considering adopting a separate board risk committee. That alternative model is in the minority, even in the financial services sector.
The separate board risk committee model has some significant problems and may inhibit the benefits from effective knowledge management.

**Separate Board Risk Committees**

This alternate model has been adopted by 17% of companies. Problems were identified with this model by both survey respondents and those interviewed. This arrangement was stronger in the financial services and the consumer products sectors.

From a practical point of view, once the shortcomings of a separate board risk committee are made transparent, boards might want to reconsider using that model.

Losing the synergies between audit and risk, reviewing the annual accounts in isolation from risk matters and failure to leverage off KM might dampen enthusiasm for the separate board risk committee as it is likely to reduce competitive advantage.

To the author’s knowledge, this is the first work, both within and outside Australia that explains the problems associated with a separate board risk committee.

**No Board Risk Committee**

The study found that 10% of S&P/ASX 200 companies have no board risk committee. The executives controlling these companies claimed that either the full board or an executive committee administered risk management.

There has been no prior research on companies that have no board risk committee therefore this finding contributes to our understanding of board governance.
The practical value of this finding is in the small percentage of companies and the size of these companies. While the no risk committee model may be appropriate in the early stages of development, a board would need to think carefully before adopting such a model in the longer term, effectively distancing themselves from better governance practices.

**Skill, Timing and Workload Issues**

This research indicates a different story in Australia which contradicts Fraser and Henry (2007), Zaman (2001) and Spira and Page (2002). In general, the S&P/ASX 200 Australian companies are not experiencing the difficulty noted in the overseas literature with finding skilled directors and finding sufficient time at committee meetings to deal with both financial and risk matters. This is an important contribution to the literature as it runs counter to the findings of overseas writers.

This finding is significant for companies struggling with finding sufficient time at audit committees to deal with both audit and risk matters. Those companies should tailor each meeting to cover either risk or audit matters and adjust the number of meetings to meet the workload.

The finding is also useful for those companies thinking of setting up a separate board risk committee to cope with timing issues. Increasing the number of board audit committee meetings, or increasing the length of each are viable alternatives.

**Enterprise Risk Management**

The survey work sought to establish the status of ERM implementation across the S&P/ASX 200 companies.
This type of maturity evaluation has been completed overseas (Beasley et al, 2005, Kleffner et al, 2003, Colquitt et al, 1999 and Miccolis et al, 2001) but to the author’s knowledge, no such metric has been attempted in Australia.

This is the first time that Australian companies have been assessed for ERM implementation status. These results can now be compared with the overseas experience. These findings enhance the literature by adding the Australian version to an international metric. It is also clear that ERM is important to leading Australian companies.

In the author’s view, this finding has a practical application for Australian companies. ERM is here and here to stay.

Ignoring ERM is no longer an option particularly with the advent of the COSO ERM Framework, AUS/NZ 4360:2004, ISO 31000:2009 and the ASX Principles. Shareholders of publically listed companies, seeking sound agency controls, will look to the risk management framework for evidence of good governance.

Directors of companies that fail, cannot afford to bring weak risk systems before courts that are seeking higher duties of care from directors.

**Executive Oversight for Risk Management**

One of the gaps in the literature, noted in Chapter Two, was the lack of research in Australia regarding executive oversight of risk management.

To the author’s knowledge, there has been no prior study on the executive oversight of risk management in Australia. These findings will help organisations decide whether they need to appoint a CRO or can use the existing CFO in the risk management role.

This has implications for professional associations, training and for education curriculum. The skill set for a CRO can be quite different from a CFO.
Integration at the Functional Level

Respondents to the survey reported that thirty percent of S&P/ASX 200 companies had combined risk management and internal audit at the operational level. This finding aligns with and extends the international literature (Walker et al, 2002 and McNamee and Selim, 1998) where audit and risk are moving closer together.

Fifty six percent of survey respondents stated that internal audit and risk management are separated at the functional level, primarily due to independence concerns.

However, the interviews with senior executives indicated that at least half of this fifty six percent had both internal audit and risk management reporting to a single executive.

The above findings contribute to the literature on the integration between internal audit and risk management. To date, that literature has focused on the areas where internal audit and risk management can, under IIA rules, work together. The independence concern has always been a stumbling block.

However, it appears that, in the S&P/ASX 200, at least thirty percent, and up to sixty percent, favour the practicalities of integration over independence. The author is hopeful that this work will encourage others to study and write on this integration, investigating whether the audit profession needs to embrace some very significant change.

Integration is an important finding for those setting up either a risk management or internal audit function. Combining internal audit with the risk function saves on costs, strengthens internal controls and allows for leverage between these two similar disciplines. However, to benefit from these synergies, the company needs to have the maturity to deal with the internal audit independence issue.
This finding is also of interest to professional associations. The increasing level of integration between audit, risk and compliance will ultimately lead to the professional associations working more closely together. A growing integration between internal audit and risk management will impact on training provided by professional bodies and curriculum at educational institutions.

**Outsourcing of Internal Audit**

This study found that eighty two percent of S&P/ASX 200 companies have an internal audit function. This is a huge increase over previous studies of the larger Australian corporate population. These larger studies found that only a third of companies had an internal audit function.

The practical implication is that leading Australian companies now consider having an internal audit function as important.

This study also found that approximately thirty percent of leading Australian companies outsource their internal audit function. This supports previous studies.

Eighteen percent of S&P/ASX 200 companies have no internal audit function. These companies conducted internal audit activities in other guises, such as through the risk management, compliance or continual improvement functions. This finding is important to the IIA and audit profession. Those bodies have been lobbying for mandatory internal audit under the ASX Principles and under company law.

Using a de-facto internal audit indicates a breaking free of the traditional internal audit world in favour of a different model. This finding has implications for the internal audit profession. If companies are drifting away from the traditional independence model, the IIA will need to either lobby for mandating internal audit through the ASX principles, or embrace the alternatives as a change in future direction.
Models for Managing Risk

The research categorised thirty five organisational charts, provided by interviewees, into four groups:

The Traditional Independence Model
The Current Merged Model
The Emerging Model
The No Internal Audit Model

There has been no previous literature on the models for managing risk either in Australia or overseas. This is the first study that has attempted to identify the structures that leading Australian companies are using to govern risk management.

These models have a practical implication for Australian companies. Companies can compare these models to their existing structure and determine whether value adding changes could be considered. New companies or companies about to adopt risk management, can choose a model that best suits their corporate culture, budget, maturity and strategy.

The study found, from interviews, that mature organisations do not require internal audit to be strictly independent. This finding has implications for the audit profession, because the independence requirement is a cornerstone of internal audit philosophy. Also, the processes implemented in the above models to overcome audit independence concerns would be worth investigation.

These processes include risk managers reporting to the chair of the audit committee, Chinese walls and the outsourcing of conflicted audits.

Contribution to the Literature

Finally the research has contributed to the literature in the form of twelve articles, each drawn from the findings, of which nine have been published at the time of writing. These articles are outlined as follows:


In Progress

<table>
<thead>
<tr>
<th>#</th>
<th>Title</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>The integration of internal audit and risk management in leading</td>
<td>Outlines the findings on integration between internal audit and risk management. Completed and accepted for publishing.</td>
</tr>
<tr>
<td></td>
<td>Australian companies</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Why Australian companies are integrating internal audit and risk</td>
<td>A good form academic article written from the synergy theory developed in the thesis. In progress.</td>
</tr>
<tr>
<td></td>
<td>management.</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>The integration of risk management and internal audit: an example of</td>
<td>A good form academic article written from the knowledge theory developed in the thesis. In progress.</td>
</tr>
<tr>
<td></td>
<td>knowledge management</td>
<td></td>
</tr>
</tbody>
</table>

Figure 5.5 Articles planned for 2014.

5.13 CONCLUSION

The study has met the primary objective:

To examine the organisational structure that is used to facilitate risk management in leading Australian companies, including an analysis of the tensions and strengths of integrating risk management with internal audit.

If a new CEO asked advice on how to set up the risk management framework in a listed public company, this study provides good practical advice.

That advice would include:

Use the board audit committee for oversight of risk management as that model facilitates the benefits from audit and risk synergy. A separate board risk committee has problems.
Audit committee meetings during strategy / budget periods could focus on risk management. Audit committee meetings around year end can focus on accounting and audit matters. Tailor the frequency and timing of meetings to the tasks at hand.

The risk management team can report to either a CFO or a CRO unless the company is trading in risky derivatives. Derivative trading would require a CRO experienced in the middle office role.

If it hasn’t yet started, the company needs to embark on the ERM implementation journey, using both the risk managers and internal auditors to manage that process.

There can be both an internal audit and a risk management presence. Internal audit activities can be carried out under a different banner if internal audit is seen as a negative.

The internal audit and risk teams can be integrated to capture the synergies between audit and risk. Such integration also facilitates effective knowledge management.

Internal audit independence can be maintained by using Chinese walls, outsourcing arrangements and reporting lines to board committees.

If the company is mature, independence will not be an issue.
### Appendix One

**S&P/ASX 200 Companies as at 30 June 2007**

<table>
<thead>
<tr>
<th>ASX Code</th>
<th>COYNAME</th>
<th>ASX Code</th>
<th>COYNAME</th>
<th>ASX Code</th>
<th>COYNAME</th>
<th>ASX Code</th>
<th>COYNAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABC</td>
<td>ABC Learning Centres Limited</td>
<td>AES</td>
<td>A ES</td>
<td>A ES</td>
<td>A ES</td>
<td>A ES</td>
<td>A ES</td>
</tr>
<tr>
<td>ABL</td>
<td>Adelaide Bank Limited</td>
<td>AGK</td>
<td>AGL Energy Limited</td>
<td>ALB</td>
<td>A Leos Corporation Limited</td>
<td>AAM</td>
<td>A Anita Limited</td>
</tr>
<tr>
<td>ABA</td>
<td>Alico Finance Group Limited</td>
<td>ALF</td>
<td>A License Limited</td>
<td>AOS</td>
<td>A Auris Limited</td>
<td>AUS</td>
<td>A Austor United Communications Limited</td>
</tr>
<tr>
<td>AGB</td>
<td>Alico Group Limited</td>
<td>AUL</td>
<td>A US Limited</td>
<td>AHC</td>
<td>A Australian Chemicals Limited</td>
<td>AWE</td>
<td>A Australian Wide Limited Exploration Limited</td>
</tr>
<tr>
<td>AHC</td>
<td>Alico Group Limited</td>
<td>AUN</td>
<td>A Australia Limited</td>
<td>ABF</td>
<td>A Babcock and Brown Limited</td>
<td>AHB</td>
<td>A Babcock and Brown Limited</td>
</tr>
<tr>
<td>AIB</td>
<td>Alico Group Limited</td>
<td>AUS</td>
<td>A Australia Limited</td>
<td>ABO</td>
<td>A Babcock and Brown Group Limited</td>
<td>AEC</td>
<td>A Australia Post Limited</td>
</tr>
<tr>
<td>AIB</td>
<td>Alico Group Limited</td>
<td>AWA</td>
<td>A WA Limited</td>
<td>ABD</td>
<td>A Babcock and Brown Group Limited</td>
<td>AMD</td>
<td>A Auckland Limited</td>
</tr>
<tr>
<td>AIB</td>
<td>Alico Group Limited</td>
<td>AXL</td>
<td>A X Limited</td>
<td>ABE</td>
<td>A Babcock and Brown Group Limited</td>
<td>AEC</td>
<td>A Australian Through Limited</td>
</tr>
<tr>
<td>AIB</td>
<td>Alico Group Limited</td>
<td>AYZ</td>
<td>A Y Limited</td>
<td>ABE</td>
<td>A Babcock and Brown Group Limited</td>
<td>AEC</td>
<td>A Australian Through Limited</td>
</tr>
<tr>
<td>AIB</td>
<td>Alico Group Limited</td>
<td>AYQ</td>
<td>A Y Limited</td>
<td>ABE</td>
<td>A Babcock and Brown Group Limited</td>
<td>AEC</td>
<td>A Australian Through Limited</td>
</tr>
<tr>
<td>AIB</td>
<td>Alico Group Limited</td>
<td>AYR</td>
<td>A Y Limited</td>
<td>ABE</td>
<td>A Babcock and Brown Group Limited</td>
<td>AEC</td>
<td>A Australian Through Limited</td>
</tr>
<tr>
<td>AIB</td>
<td>Alico Group Limited</td>
<td>AYN</td>
<td>A Y Limited</td>
<td>ABE</td>
<td>A Babcock and Brown Group Limited</td>
<td>AEC</td>
<td>A Australian Through Limited</td>
</tr>
<tr>
<td>AIB</td>
<td>Alico Group Limited</td>
<td>AYZ</td>
<td>A Y Limited</td>
<td>ABE</td>
<td>A Babcock and Brown Group Limited</td>
<td>AEC</td>
<td>A Australian Through Limited</td>
</tr>
<tr>
<td>AIB</td>
<td>Alico Group Limited</td>
<td>AYQ</td>
<td>A Y Limited</td>
<td>ABE</td>
<td>A Babcock and Brown Group Limited</td>
<td>AEC</td>
<td>A Australian Through Limited</td>
</tr>
<tr>
<td>AIB</td>
<td>Alico Group Limited</td>
<td>AYR</td>
<td>A Y Limited</td>
<td>ABE</td>
<td>A Babcock and Brown Group Limited</td>
<td>AEC</td>
<td>A Australian Through Limited</td>
</tr>
<tr>
<td>AIB</td>
<td>Alico Group Limited</td>
<td>AYN</td>
<td>A Y Limited</td>
<td>ABE</td>
<td>A Babcock and Brown Group Limited</td>
<td>AEC</td>
<td>A Australian Through Limited</td>
</tr>
<tr>
<td>AIB</td>
<td>Alico Group Limited</td>
<td>AYZ</td>
<td>A Y Limited</td>
<td>ABE</td>
<td>A Babcock and Brown Group Limited</td>
<td>AEC</td>
<td>A Australian Through Limited</td>
</tr>
<tr>
<td>ASX</td>
<td>CIGS</td>
<td>REV</td>
<td>AUDRISK</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>------</td>
<td>-----</td>
<td>---------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ABS</td>
<td>25</td>
<td>1,696</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ADB</td>
<td>65</td>
<td>335</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ABCG</td>
<td>15</td>
<td>791</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AGK</td>
<td>55</td>
<td>3,765</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ALS</td>
<td>20</td>
<td>738</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AAN</td>
<td>55</td>
<td>1,482</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AFG</td>
<td>65</td>
<td>546</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AWC</td>
<td>15</td>
<td>569</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AMC</td>
<td>15</td>
<td>10,872</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AMP</td>
<td>65</td>
<td>2,416</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ANN</td>
<td>35</td>
<td>800</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>APA</td>
<td>55</td>
<td>533</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>APN</td>
<td>25</td>
<td>1,293</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A2Z</td>
<td>60</td>
<td>121</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AGP</td>
<td>15</td>
<td>709</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ALL</td>
<td>25</td>
<td>1,100</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AOE</td>
<td>10</td>
<td>28</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AJO</td>
<td>20</td>
<td>2,750</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ASX</td>
<td>65</td>
<td>553</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AUN</td>
<td>25</td>
<td>503</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ALZ</td>
<td>65</td>
<td>1,058</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ANZ</td>
<td>65</td>
<td>25,510</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AOC</td>
<td>20</td>
<td>186</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AUW</td>
<td>65</td>
<td>286</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AWE</td>
<td>10</td>
<td>144</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AWR</td>
<td>35</td>
<td>4,854</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AXA</td>
<td>65</td>
<td>2,806</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BBI</td>
<td>55</td>
<td>1,239</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BNB</td>
<td>65</td>
<td>1,293</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BBP</td>
<td>55</td>
<td>4</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BBW</td>
<td>55</td>
<td>104</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BCD</td>
<td>65</td>
<td>2,904</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BJT</td>
<td>60</td>
<td>76</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BDG</td>
<td>65</td>
<td>1,811</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BPT</td>
<td>10</td>
<td>567</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BEN</td>
<td>65</td>
<td>1,263</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BHP</td>
<td>15</td>
<td>59,341</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BBG</td>
<td>25</td>
<td>1,230</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BSL</td>
<td>15</td>
<td>8,164</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BLY</td>
<td>20</td>
<td>1,825</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BSG</td>
<td>15</td>
<td>0</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BOL</td>
<td>20</td>
<td>350</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BLK</td>
<td>15</td>
<td>4,909</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BKN</td>
<td>20</td>
<td>640</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BBX</td>
<td>20</td>
<td>3,868</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BHP</td>
<td>60</td>
<td>60</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CAB</td>
<td>20</td>
<td>152</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CTX</td>
<td>10</td>
<td>18,665</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CLO</td>
<td>15</td>
<td>902</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CNP</td>
<td>60</td>
<td>795</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix Three – Survey Instrument

The Governance of Risk Management in Leading Australian Companies

A study of S&P / ASX 200 leading Australian companies to determine the corporate governance placed over risk management at both board committee and operational levels

Principal Researcher: Steven Halliday (03 62 305316) 0417 573 559 steven.halliday@hydro.com.au

Authorised by: Charles Sturt University

Supported by: Hydro Tasmania

Survey Participant: XYZ Company Limited

Respondent: John Citizen
The survey consists of twelve questions and will take between ten and fifteen minutes to complete. All respondents will receive a copy of the completed dissertation (by email or CD) which will be very useful for benchmarking or comparing risk management arrangements in Australia.

PLEASE START HERE

PART A – Questions 1 and 2 are introduction questions

Question One – Demographic Information

Please indicate your company’s approximate revenue in Australian dollars at the consolidated level? For example [AUD$680m]

AUD$m..........................................................................................

Question Two – Maturity of Enterprise Risk Management (ERM)

On a scale of 1 – 5, please indicate the extent of adoption of Enterprise Risk Management (ERM) in your organisation by circling one of the numbers below

Rejection/Unaware of ERM  1……2……3……4…….5  Fully Mature ERM

Comments………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………

PART B – Questions 3 to 6 relate to the oversight of risk management at board committee level

Question Three – At the board committee level.

How is risk management governed in your organisation at board committee level? Please tick one box below?

The board audit committee deals with risk management (please go to question four)

A specific board risk committee exists, separate from the board audit committee (please skip to question six)

No risk committee at board committee level (please skip to question seven)

Other (please specify below)

Comments…………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………


Question Four – For combined board audit and risk committees

If your board risk committee is separate from the audit committee, please go to question six.
If your company has no risk committee at board level, please go to question seven.

If your board audit committee is combined with your board risk management committee, why was such a model chosen? Please indicate the importance of each of the following decision criteria by circling a number.

(a) High cost of board committees
   Not Important 1……2……3……4……5 Very Important

(b) Convenient to have a single committee
   Not Important 1……2……3……4……5 Very Important

(c) We have adopted what we consider is the industry standard model
   Not Important 1……2……3……4……5 Very Important

(d) This company is too small to have separate board audit and risk committees
   Not Important 1……2……3……4……5 Very Important

(e) Audit work and Risk management have natural synergies
   Not Important 1……2……3……4……5 Very Important

Please describe any other reasons for your organisation having a combined board audit and risk committee and score those reasons from 1 to 5.

...................................................................................................................................................
...................................................................................................................................................
...................................................................................................................................................
...................................................................................................................................................
...................................................................................................................................................
...................................................................................................................................................
...................................................................................................................................................
...................................................................................................................................................
...................................................................................................................................................
...................................................................................................................................................
...................................................................................................................................................
...................................................................................................................................................
...................................................................................................................................................
...................................................................................................................................................
...................................................................................................................................................
...................................................................................................................................................
...................................................................................................................................................
...................................................................................................................................................
...................................................................................................................................................
...................................................................................................................................................
................................................................................................................................................... Please go to question five
Question Five – For combined board audit and risk committees

If your board risk committee is separate from the audit committee, please go to question six.
If your company has no risk committee at board level, please go to question seven.

Writers in the United Kingdom and Australia have suggested that combined board audit and risk committees may be faced with the following problems:

1. Finding directors who have both financial and risk management skills; and
2. Finding enough time at audit committee meetings to deal with both financial matters and risk issues

Please indicate the relevance of each of the following issues by circling an appropriate number

(a) Issues finding directors with both Risk Management and Financial skills
   No Problems 1........2........3........4........5 Significant Problems

(b) Issues finding directors with Risk Management skills
   No Problems 1........2........3........4........5 Significant Problems

(c) Issues finding directors with Financial skills
   No Problems 1........2........3........4........5 Significant Problems

(d) Issue of finding enough time at Audit Committee meetings to deal with both financial and risk management matters
   No Problems 1........2........3........4........5 Significant Problems

Are there any comments you can make on how your organisation is dealing with the above issues.

...........................................................................................................................................................................
...........................................................................................................................................................................
...........................................................................................................................................................................
...........................................................................................................................................................................
...........................................................................................................................................................................
...........................................................................................................................................................................
...........................................................................................................................................................................
...........................................................................................................................................................................

Please go to question seven
Question Six – For separate board risk committee (separate from audit committee)

For companies with combined board audit and risk committees or no board risk committee, please go to question seven.

If you have set up a separate board risk committee (separate from the audit committee) why was such an arrangement chosen? Please indicate the importance of each of the following decision criteria by circling an appropriate number.

(a) To manage specific financial risks
   Not Important 1........2........3........4........5 Very Important

(b) To assist with Enterprise Risk Management (ERM) adoption
   Not Important 1........2........3........4........5 Very Important

(c) This arrangement is preferred by our regulator
   Not Important 1........2........3........4........5 Very Important

(d) We have adopted what we consider is the industry standard model
   Not Important 1........2........3........4........5 Very Important

(e) The separate risk committee has evolved over time from former credit and financial risk committees
   Not Important 1........2........3........4........5 Very Important

(f) The company operates in a high profile area and a separate risk committee is used to portray a strong focus on risk management
   Not Important 1........2........3........4........5 Very Important

Please describe any other reasons for your organisation having a separate Board Risk Committee and score those reasons from 1 to 5.

...........................................................................................................
...........................................................................................................
...........................................................................................................
...........................................................................................................
...........................................................................................................
...........................................................................................................
...........................................................................................................
...........................................................................................................

Please go to question seven
PART C – Questions 7 to 12 relate to the oversight of risk management at the executive and operational levels

Question Seven – At the executive level

Which executive officer is responsible for risk management at the operational level? Please tick one box below.

□ Chief Risk Officer
□ Chief Executive Officer
□ Chief Finance Officer
□ Chief Audit Executive
□ Company Secretary
□ Combined Audit and Risk Executive
□ Other (please specify below)

Comments……………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………

Question Eight – At the operational level

How is your organisation’s risk management function arranged at the operational or functional level? Please tick one box below.

□ Risk management function is combined with internal audit (please skip to question ten)
□ Risk management function is separate from internal audit (please move on to question nine)
□ Risk management function is outsourced (please skip to question twelve)
□ No risk management function (please skip to question twelve)
□ Other (please specify below)

Comments……………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………


Question Nine – For companies with separate risk management functions at the operational level

Companies with combined internal audit and risk management functions, please go to question ten. If you have no risk management function at the operational level, please go to question twelve (the last question).

If you have established a separate risk management function (separate from Internal Audit) at the operational level, why was such a model chosen? Please indicate the importance of each of the following issues by circling an appropriate number

(a) Internal audit is outsourced
   Not Important 1........2........3........4........5  Very Important

(b) Internal audit must remain independent from risk management
   Not Important 1........2........3........4........5  Very Important

(c) We see no strong links between internal audit and risk management
   Not Important 1........2........3........4........5  Very Important

(d) One of our existing executive managers (not the Chief Audit Executive) has accepted responsibility for risk management
   Not Important 1........2........3........4........5  Very Important

(e) Because we have a separate risk management committee at board level
   Not Important 1........2........3........4........5  Very Important

(f) There is no particular reason for this arrangement, the current set-up evolved over time
   Not Important 1........2........3........4........5  Very Important

Please describe any other reasons for your organisation having a separate risk management function at the operational level and score that reason from 1 to 5

................................................................................................................................................
................................................................................................................................................
................................................................................................................................................
................................................................................................................................................
................................................................................................................................................
................................................................................................................................................
................................................................................................................................................
................................................................................................................................................

Please go to question twelve (the last question)
Question Ten – For combined internal audit and risk management functions at the operational level

If your company has a risk management function that is separate from internal audit at the operational level, or no risk management function, please go to question twelve (the last question).

If your organisation has a combined internal audit and risk management function at the operational level, why was that model chosen? Please indicate the importance of each of the following issues by circling an appropriate number

(a) To save costs
   Not Important 1…….2…….3…….4…….5 Very Important

(b) Internal audit and risk management are both internal controls
   Not Important 1…….2…….3…….4…….5 Very Important

(c) We have adopted what we consider is the industry standard model
   Not Important 1…….2…….3…….4…….5 Very Important

(d) This company is too small to have separate audit and risk functions
   Not Important 1…….2…….3…….4…….5 Very Important

(e) Internal audit and risk management have natural synergies
   Not Important 1…….2…….3…….4…….5 Very Important

Please describe any other reasons for your organisation having a combined internal audit and risk management function at the operational level and score that reason from 1 to 5

...................................................................................................................................................
...................................................................................................................................................
...................................................................................................................................................
...................................................................................................................................................
...................................................................................................................................................
...................................................................................................................................................
...................................................................................................................................................
...................................................................................................................................................
...................................................................................................................................................
...................................................................................................................................................
...................................................................................................................................................

Please go to question eleven
Question Eleven – For combined internal audit and risk management functions at the operational level

*If your company has a risk management function that is separate from internal audit at the operational unit, or no risk management function, please go to question twelve (the last question).*

*If your organisation has a combined internal audit and risk management function at the operational level, how do you deal with independence issues? Such issues can occur when internal audit is required to audit the risk management area. Please tick the relevant box below.*

- □ We do not see independence as an issue
- □ We outsource the auditing of risk management areas to external firms
- □ We establish “Chinese walls” by keeping a dedicated internal auditor separated from risk management
- □ Other (please specify below)

Comments
...........................................................................................................................................  
...........................................................................................................................................

Question Twelve – At the operational level

*Some internal audit functions are run by a Chief Audit Executive, who manages either a small in-house audit team or a co-sourced arrangement with external providers. Other companies outsource their entire internal audit function to external providers and have another executive (for example the Chief Finance Officer or Company Secretary) manage that external contractual relationship. Please tick the box that best describes your company’s arrangements?*

- □ A co-sourced internal audit function (managed by a Chief Audit Executive)
- □ An outsourced internal audit function (managed by another executive)
- □ No internal audit function
- □ Other (please specify below)

Comments.........................................................................................................................................
...........................................................................................................................................
...........................................................................................................................................

End of Survey – thank you for your participation

*If you would be prepared to participate in a short (10 minute) telephone interview please complete the section on the next page.*
Involvement in Short Interview

If you would be prepared to participate in a short telephone interview to further discuss and clarify issues related to this study, please indicate your willingness by providing your e-mail address below.

The interviews will be preceded by an e-mail outlining the proposed questions and would be conducted by the principal researcher using a recorded telephone line. The actual interview will be transcribed and emailed to you within 2 days of conducting the interview.

I am prepared to be involved in a short interview which I acknowledge by providing my e-mail address below.

E-mail address………………………………………………………………………………

Thank you again for your contribution to this research
### Appendix Four

**Survey Response Database – First 51 Responses**

| Col1 | Col2 | Col3 | Col4 | Col5 | Col6 | Col7 | Col8 | Col9 | Col10 | Col11 | Col12 | Col13 | Col14 | Col15 | Col16 | Col17 | Col18 | Col19 | Col20 | Col21 | Col22 | Col23 | Col24 | Col25 | Col26 | Col27 | Col28 | Col29 | Col30 | Col31 | Col32 | Col33 | Col34 | Col35 | Col36 | Col37 | Col38 | Col39 | Col40 | Col41 | Col42 | Col43 | Col44 | Col45 | Col46 | Col47 | Col48 | Col49 | Col50 | Col51 |
|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|
## Appendix Four

### Survey Response Database – Second 51 Responses

<table>
<thead>
<tr>
<th>Response</th>
<th>Frequency</th>
<th>Response</th>
<th>Frequency</th>
<th>Response</th>
<th>Frequency</th>
<th>Response</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,429</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>1,000</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>1,408</td>
<td>5</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>205</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>7,805</td>
<td>6</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>205</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1,000</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>1,429</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1,000</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>1,408</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>200</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>1,000</td>
<td>5</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>1,408</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>200</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1,000</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>1,429</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1,000</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>1,408</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>200</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1,000</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>1,429</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1,000</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>1,408</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>200</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1,000</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>1,429</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1,000</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>1,408</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>200</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1,000</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>1,429</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1,000</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>1,408</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>200</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1,000</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>1,429</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1,000</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>1,408</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>200</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1,000</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>1,429</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1,000</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>1,408</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>200</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1,000</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>1,429</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1,000</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>1,408</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>200</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1,000</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>1,429</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1,000</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>1,408</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>200</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1,000</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>1,429</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1,000</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>1,408</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>200</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>RESEARCH OBJECTIVE ONE</td>
<td>INCLUDES</td>
<td>SURVEY AND INTERVIEW QUESTIONS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td>----------</td>
<td>-------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Combined board committees</td>
<td>1. Approximate revenue? (SQ1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Separate board committees</td>
<td>2. Maturity of Enterprise Risk Management? (SQ2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Problems with skill, workload and timing</td>
<td>3. How is risk management governed at the board committee level? (SQ3)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Executive management</td>
<td>4. Why was a combined board audit and risk committee chosen? (SQ4)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Functional or operational level</td>
<td>5. Are you having difficulty finding skilled directors and finding enough time for both audit and risk consideration at board committee meetings? (SQ5)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>No board risk committee</td>
<td>6. Why was a separate board risk management committee chosen? (SQ6)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Synergies</td>
<td>7. Which executive officer is responsible for risk management at the operational level? (SQ7)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**STRUCTURE:**
To investigate the structure of risk management at the board, executive and operational levels in leading Australian companies.

8. How is your risk management function arranged at the operational level? (SQ8)
9. If risk management is separated from internal audit, why was that model chosen? (SQ9)
10. If risk management is combined with internal audit, why was that model chosen? (SQ10)
**RESEARCH OBJECTIVE TWO**

**INCLUDES**

**INTEGRATION:**
To explore the levels of integration between internal audit and risk management in leading Australian companies.

<table>
<thead>
<tr>
<th>Integration</th>
<th>Synergies</th>
<th>Specific business risks</th>
<th>Auditor independence</th>
<th>Integration at executive level</th>
<th>Integration at the functional level</th>
<th>No internal audit</th>
<th>No risk management</th>
<th>Outsourcing and co-sourcing</th>
</tr>
</thead>
</table>

**SURVEY AND INTERVIEW QUESTIONS**

<table>
<thead>
<tr>
<th>SQ (Survey Question)</th>
<th>IQ (Interview Question)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Can you please elaborate on the synergies that link internal audit to risk management? (IQ1)</td>
<td></td>
</tr>
<tr>
<td>2. Your separate board risk committee focuses on specific business risks. Can you elaborate on the importance of these issues? (IQ2)</td>
<td></td>
</tr>
<tr>
<td>3. How are you dealing with the problem of finding sufficient time at board audit committee meetings to deal with both risk and audit? (IQ3)</td>
<td></td>
</tr>
<tr>
<td>4. Do you see any evidence of integration between internal audit and risk management across Australian companies? (IQ4)</td>
<td></td>
</tr>
<tr>
<td>5. How does your combined internal audit and risk management function deal with independence issues? (SQ11) (IQ5)</td>
<td></td>
</tr>
<tr>
<td>6. You do not have an internal audit function. How do you cover assurance and governance matters? (IQ6)</td>
<td></td>
</tr>
<tr>
<td>7. You do not have a risk management committee. How do you meet ASX Principle number seven? (IQ7)</td>
<td></td>
</tr>
<tr>
<td>8. What are your internal audit arrangements with respect to outsourcing and co-sourcing? (SQ12)</td>
<td></td>
</tr>
<tr>
<td>9. Do you see internal audit as a subset of risk management? (IQ8)</td>
<td></td>
</tr>
</tbody>
</table>
### RESEARCH OBJECTIVE THREE

**MODELS:**

To outline the significant models being used by Australian companies for risk management and investigate options for the future.

<table>
<thead>
<tr>
<th>INCLUDES</th>
<th>DETERMINANTS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>COVERS</strong></td>
<td>1. Board committee arrangements.</td>
</tr>
<tr>
<td>Traditional independence model</td>
<td>2. Executive oversight of risk management.</td>
</tr>
<tr>
<td>Current merged model</td>
<td>3. Reliance on independence.</td>
</tr>
<tr>
<td>Emerging model</td>
<td>4. Maturity of the organisation.</td>
</tr>
<tr>
<td>No internal audit model</td>
<td>5. Involvement in strategic planning.</td>
</tr>
<tr>
<td></td>
<td>6. Forward versus backward orientation.</td>
</tr>
<tr>
<td></td>
<td>7. The existence of an internal audit function.</td>
</tr>
</tbody>
</table>
Appendix Six

Are audit committees in control of risk management?

Do audit committees have the necessary skills to undertake the implementation of enterprise risk management, asks Steve Halliday

The losses recently incurred by Société Générale as the result of a "rogue trader" only confirm the stance taken by the Australian Securities Exchange (ASX) Corporate Governance Council last year, which requires that Australian listed companies strengthen their risk management efforts. The first completed section of a research project into the governance of risk management in leading Australian companies has found that risk management, or more correctly, enterprise risk management (ERM), while still trying to find its place in the Australian corporate entity, has largely been placed under the custody of the audit committee.

Over the past 10 years, enterprise risk management has become firmly embedded on the corporate governance agenda. With origins in the insurance, occupational health and safety industries, the rise of risk management has been fuelled by regulatory responses to the international corporate collapses experienced over the past decade. In the United States, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management Framework highlighted risk management as a material issue in the United Kingdom, the Turnbull Report succeeded in bringing risk management to the board table.

In Australia, the risk management standard AUS/NZS 4360:2004 has become the benchmark for risk management, to such an extent that many overseas countries have adopted that standard. The original ASX Principles of Good Corporate Governance introduced risk management in a governance context and recent revisions to those principles have strengthened the risk management requirements for listed companies.

Indeed, the impact of these regulations plus increased director liability, shareholder activism and the influence of institutional investors have all contributed to an increased focus on risk management. This is clearly evidenced by the fact that Standard & Poor's (S&P) now rank the governance of risk management into account for ratings purposes thereby potentially affecting a firm's cost of capital.

The study upon which this article is based looks at the governance of risk management at board committee level and at functional level in Australian companies and seeks to flesh out the issues that are associated with the risk management discipline coming of age.

Take control of your career. Now!

Like most internal audit professionals, you're probably thinking how to move your career forward. How to be better at what you do. How to jump ahead and be noticed. The qualification Certified Internal Auditor is the only internationally accepted qualification for internal auditors.

To book or for more information go to www.iia.org.au or phone
Julie Young on 1800 236 266 or 02 9287 9155
It appears, at first glance, that these companies are saying that normal board governance processes equate to a sound risk management process.

They tended to be a mix of smaller mining start-up companies, where risk management had not matured, or listed property trusts affiliated with a larger organisation that may be providing the risk oversight. Interestingly, these smaller companies, with no board risk committee, are still required to comment on ASX governance principle number seven (recognise and manage risk) in their annual reports.

In some cases, these smaller companies stated that they have sound risk management processes, namely: (1) the directors are picked using a robust process; (2) the executive management team is skilled; and (3) important issues are discussed at board level.

In these cases, the term ERM was not mentioned, there appeared to be no chief risk officer and the ASX/NZSE 4300:2004 standard was not quoted as a benchmark.
Appendix Seven

Survey Pre-notification Letter

Dear

I am currently completing doctoral research on the governance of risk management in leading Australian companies. This is the first time such research has been undertaken in Australia and the outcome will help companies establish what “good practice” looks like in this emerging area. This work is being supervised by Charles Sturt University and is supported by my employer, Hydro Tasmania.

In May 2008, I will be sending you a short (twelve question) survey and I am seeking your support for the project by asking you to spend about 15 minutes to complete and return the survey. All respondents will receive a copy of the completed dissertation (by email or CD) which will assist you with your governance endeavours.

If you have any queries or concerns, please contact me on 03 62 305316 or by e-mail, steven.halliday@hydro.com.au

Thank you for your assistance with this important project.

Steven Halliday

Group Manager Assurance

Hydro Tasmania

GPO Box 355

Hobart, TASMANIA 7001
Appendix Eight

Information Statement

30 June 2008
Mr John Citizen
Chief Risk Officer
XYZ Limited
200 Spencer St
MELBOURNE, Victoria, 3000

Dear John

INFORMATION STATEMENT

The Governance of Risk Management in Leading Australian Companies

Please allow me to introduce myself and the research which I am currently undertaking. My name is Steven Halliday and my role is that of Group Manager Assurance with Hydro Tasmania, the Tasmanian state owned electricity generator. I report to the Corporation Secretary.

I am currently enrolled with Charles Sturt University and undertaking a Doctorate in Business Administration. Broadly, the research looks at the board committee and management structures over risk management in leading Australian companies. This is the first time such research has been undertaken and the models being used in Australia will be extracted and published from the research. This will establish a “good practice” benchmark for company’s to use when benchmarking risk management.

The study is being undertaken in three sections, the first of which has been completed:

- Stage One – desktop analysis of S&P / ASX 200 (looking at board committee structures);
- Stage Two – short survey of S&P / ASX 200 (looking at board committee and operational structures); and
- Stage Three – brief interviews with Company Secretaries of a number of S&P / ASX 200 companies to flesh out queries from the above.

Request for Involvement

As the leading governance professional in your company, I am seeking your support for the project by asking you to spend about 15 minutes to complete and return the attached survey. All respondents will receive a copy of the completed dissertation (by email or CD) which will be very useful for benchmarking or comparing risk management arrangements in Australia.
Confidentiality

The most significant risk to survey participants is one of breaching confidentiality. The surveys will be conducted under the rules established by Charles Sturt University Ethics Committee. Neither your identity nor the identity of your organisation will be discussed in the research as all results and opinions will be aggregated. No confidential information will appear in any publication related to this research. All documentation will be kept under lock and key in a secure office and destroyed after five years – to comply with legislative requirements. You will receive a copy of the final research report (by email or on compact disc) once the work is completed.

My contact details, and those of my supervisors are attached and the paragraph below is provided to you for added assurance over this project.

**NOTE** : Charles Sturt University’s Ethics in Human Research Committee has approved this project. If you have any issues, questions or reservations about the ethical conduct of this project, you may contact the Committee through the Executive Officer:

The Executive Officer  
Ethics in Human Research Committee  
Academic Secretariat  
Charles Sturt University  
Private Mail Bag 29  
Bathurst N.S.W.  2795  
Tel: (02) 6338 4628  
Fax: (02) 6338 4194

Thank you for taking the time to read this information statement. If you would assist by completing the attached survey and returning in the envelope provided. If you wish to make contact, please complete the survey, scan and email the survey to steven.halliday@hydro.com.au. That will establish a dialogue to assist with any clarification and allow a potential future telephone interview to discuss any issues.

Thanks for helping make this project meaningful for Australian Company Secretaries.

Yours faithfully

Steven Halliday  
Principal Investigator
CONTACT DETAILS FOR RESEARCHER AND SUPERVISORS

Principal Investigator
Student No 11330648
Steven Halliday
Group Manager Assurance
Hydro-Electric Corporation
4 Elizabeth Street
Hobart Tasmania 7000
Tel:  (03) 62 30 5316
Email:  steven.halliday@hydro.com.au

Supervisor
Roderick Duncan
Lecturer
School of Marketing and Management
Charles Sturt University
Panorama Ave
Bathurst N.S.W.  2795
phone + 61 2 63384982
fax + 61 2 63384649

Supervisor
Kay Plummer
Associate Head of School & Courses Manager,
School of Accounting and Computer Science
Charles Sturt University
Panorama Ave
Bathurst NSW  2795
phone + 61 2 63384447
fax + 61 2 63384649
Appendix Nine – Survey Reminder

Date

Mr John Citizen
Group Chief Risk Officer
XYZ Limited
200 Pitt St
Sydney, NSW 2000

Dear John

SURVEY REMINDER

The Governance of Risk Management in Leading Australian Companies

In late May / early June 2008 you received a survey relating to the board committee and management structures over risk management in leading Australian companies. Since a response has not yet been received from your organisation a copy of the survey and a return envelope is attached in case you have mislaid or you failed to receive the original survey. If you have already completed the survey please disregard this letter and thank you for your support.

Support

Could you please complete the attached survey and return in the envelope provided. It should only take 10 – 15 minutes. In return all respondents will be provided with a copy of the completed research report which will establish a “good practice” benchmark for Australian companies to use when benchmarking risk management activities.

Confidentiality

The survey is being conducted under the rules established by Charles Sturt University Ethics Committee. Neither your identity nor the identity of your organisation will be discussed in the research as all results and opinions will be aggregated. No confidential information will appear in any publication related to this research.

Thanks for your help to make this project meaningful for Australian Company Secretaries.

Yours faithfully

Steven Halliday
Principal Investigator
Appendix Ten – Frequency Tables

Frequency Tables for Survey Data-set Analysis

[Dataset2] D:\D\Doctorate\Research Instruments\Survey.sav

<table>
<thead>
<tr>
<th></th>
<th>CIGS</th>
<th>ERM</th>
<th>ADR</th>
<th>EXO</th>
<th>FUN</th>
<th>IAU</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>102</td>
<td>102</td>
<td>102</td>
<td>102</td>
<td>102</td>
<td>102</td>
</tr>
<tr>
<td>Missing</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Frequency Table

**CIGS**

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td>10</td>
<td>11</td>
<td>10.8</td>
<td>10.8</td>
</tr>
<tr>
<td>15</td>
<td>22</td>
<td>21.6</td>
<td>21.6</td>
<td>32.4</td>
</tr>
<tr>
<td>20</td>
<td>8</td>
<td>7.8</td>
<td>7.8</td>
<td>40.2</td>
</tr>
<tr>
<td>25</td>
<td>15</td>
<td>14.7</td>
<td>14.7</td>
<td>54.9</td>
</tr>
<tr>
<td>30</td>
<td>6</td>
<td>5.9</td>
<td>5.9</td>
<td>60.8</td>
</tr>
<tr>
<td>35</td>
<td>4</td>
<td>3.9</td>
<td>3.9</td>
<td>64.7</td>
</tr>
<tr>
<td>45</td>
<td>1</td>
<td>1.0</td>
<td>1.0</td>
<td>65.7</td>
</tr>
<tr>
<td>50</td>
<td>2</td>
<td>2.0</td>
<td>2.0</td>
<td>67.6</td>
</tr>
<tr>
<td>55</td>
<td>7</td>
<td>6.9</td>
<td>6.9</td>
<td>74.5</td>
</tr>
<tr>
<td>60</td>
<td>10</td>
<td>9.8</td>
<td>9.8</td>
<td>84.3</td>
</tr>
<tr>
<td>65</td>
<td>16</td>
<td>15.7</td>
<td>15.7</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>102</td>
<td>100.0</td>
<td>100.0</td>
<td></td>
</tr>
</tbody>
</table>

**ERM**

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td>1</td>
<td>2</td>
<td>2.0</td>
<td>2.0</td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td>9.8</td>
<td>9.8</td>
<td>11.8</td>
</tr>
<tr>
<td>3</td>
<td>38</td>
<td>37.3</td>
<td>37.3</td>
<td>49.0</td>
</tr>
<tr>
<td>4</td>
<td>40</td>
<td>39.2</td>
<td>39.2</td>
<td>88.2</td>
</tr>
<tr>
<td>5</td>
<td>12</td>
<td>11.8</td>
<td>11.8</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>102</td>
<td>100.0</td>
<td>100.0</td>
<td></td>
</tr>
</tbody>
</table>

**ADR**

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td>0</td>
<td>1</td>
<td>1.0</td>
<td>1.0</td>
</tr>
<tr>
<td>1</td>
<td>68</td>
<td>66.7</td>
<td>66.7</td>
<td>67.6</td>
</tr>
<tr>
<td>2</td>
<td>24</td>
<td>23.6</td>
<td>23.5</td>
<td>91.2</td>
</tr>
<tr>
<td>3</td>
<td>8</td>
<td>7.8</td>
<td>7.8</td>
<td>99.0</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>1.0</td>
<td>1.0</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>102</td>
<td>100.0</td>
<td>100.0</td>
<td></td>
</tr>
<tr>
<td>EXO</td>
<td>Frequency</td>
<td>Percent</td>
<td>Valid Percent</td>
<td>Cumulative Percent</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
<td>---------</td>
<td>---------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Valid 1</td>
<td>27</td>
<td>26.5</td>
<td>26.5</td>
<td>26.5</td>
</tr>
<tr>
<td></td>
<td>19</td>
<td>18.6</td>
<td>18.6</td>
<td>45.1</td>
</tr>
<tr>
<td></td>
<td>33</td>
<td>32.4</td>
<td>32.4</td>
<td>77.5</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>9.8</td>
<td>9.8</td>
<td>87.3</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>8.8</td>
<td>8.8</td>
<td>96.1</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>3.9</td>
<td>3.9</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>102</td>
<td>100.0</td>
<td>100.0</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FUN</th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid 1</td>
<td>24</td>
<td>23.5</td>
<td>23.5</td>
<td>23.5</td>
</tr>
<tr>
<td></td>
<td>63</td>
<td>61.8</td>
<td>61.8</td>
<td>85.3</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>2.0</td>
<td>2.0</td>
<td>87.3</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>7.8</td>
<td>7.8</td>
<td>95.1</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>4.9</td>
<td>4.9</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>102</td>
<td>100.0</td>
<td>100.0</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IAU</th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid 1</td>
<td>59</td>
<td>57.8</td>
<td>57.8</td>
<td>57.8</td>
</tr>
<tr>
<td></td>
<td>25</td>
<td>24.5</td>
<td>24.5</td>
<td>82.4</td>
</tr>
<tr>
<td></td>
<td>18</td>
<td>17.6</td>
<td>17.6</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>102</td>
<td>100.0</td>
<td>100.0</td>
<td></td>
</tr>
</tbody>
</table>
Appendix 11 AUDIT & RISK SYNERGIES Interpretive Code

Company Question: You have a combined Audit and Risk Committee due to the synergies between Audit and Risk - please elaborate?

1. There is a natural flow of synergy. The outcomes (risk assessment) of strategic and operational risk management drive the Internal Audit plans. The outcome of the Internal Audit work finds more risks and tells us how we are going on risk management which both feed back into risk management (there is a circular flow diagram here). 03-01

2. In regard to synergies, I see the flip side as more important. Because Risk and Audit are so closely aligned and overlap, having separate Board Committees would cause unnecessary complications. The Board Committees would be continually competing over jurisdiction and what matters fall into what Committee's area of expertise. 03-02

3. We have an orthodox charter for the Audit Risk and Compliance Committee. The Committee receives reports on Audit Risk and Compliance matter. The Committee looks at the top 20 Operational Risk issues. For comfort, the Committee requests the outsourced Internal Audit function dive in and provide a better understanding of the risk, the mitigations and progress on a number of these risks. In this context, risk is the antenna and the outsourced IA helps with the solution. We use PWC who bring in different partners depending on the issue. For example we recently had a fraud partner assist us with our fraud control plan. Risk also has synergy with Compliance. If we have a compliance breach, a breakdown in controls, then IA dive in to ascertain the cause and effect and then put controls in place to solve the problem. With an AFSL, and APRA and ASIC, this synergy is critical. 03-01

4. We have an annual Risk Workshop, facilitated by KPMG under the auspices of the AC. The risks developed are reviewed throughout the year via management presentations to the AC. 03-02

5. The Risk Managers use the outcomes from audit activity to identify areas of higher risk, then mitigate accordingly. 03-03

6. All the risks, OH&S, HS&E, Construction, Finance and Debt are pulled together and overseen at the Board Audit Committee. These are the inputs. The culmination of managing all those risks is the financial report which is in many ways the output of the Audit Committee. 03-03

7. The ultimate aim of the Audit Committee is to deal with the financial statements. These statements are derived from the performance of the company, which is the culmination of taking opportunities and managing risk. Having RM in the AC gives the AC a more holistic view of the business opportunities, the wins and losses and ultimately helps with the integrity of the accounts. We have an annual Risk Workshop, facilitated by KPMG under the auspices of the AC. The risks developed are reviewed throughout the year via management presentations to the AC. 03-04

8. Traditionally the Audit Committee dealt with financial risk which brings in a risk perspective. Managing risk is integral to preserving over the integrity of the annual accounts in that internal controls and processes must be working properly. The Management Rep letter, which is signed by the CEO and CFO is based on systems of internal control, strong risk management and has to align with the new requirements of ASX principle no seven. 03-05

9. The Audit is about annual accounts and balance sheet but these are just the culmination (reporting) of all underlying opportunities, threats and how risks are dealt with. Tip of the iceberg model (see written interview) 03-06

10. Our IA is outsourced to E&Y. We benchmark very light on, and intend to stay so for historical and cost reasons. Synergies - the Board looks at high level risks that threaten our objectives, i.e. compliance with laws, reputation etc. Internal audit focus on those issues when conducting reviews. 03-07

11. Two main areas of synergy. Firstly the annual audit plan can be derived from audit risk view or from the RM business view - synergy helps with the latter. Secondly the electronic risk register can be a tool for Internal Audit to select controls and do their validation work. 03-08

12. Over recent years Internal Audit has been able to become more efficient and more focussed by using the full risk register to determine where to direct audit activities. 03-09

13. IA is all about internal controls. Internal controls are put in place to manage risk. The Board are interested in financial reporting controls which again are directed at managing risk. Also the ASX principles link audit and risk. 03-10

14. I does not have an internal auditor. She is the CFO. She completes the risk reviews for the organisation and keeps abreast of internal controls. When she finds a problem or issue, or a mitigation is required, she allocates the solving of that problem to either internal team members or external. She sees this cycle of Risk assessment, identify problems, appoint fixer and in some cases external validation as the Risk Management / Continual Improvement process. In this way we are not asking external experts to come in and identify issues that we already know about. Risk is the initiator and defacto audit is the fixer. This appears to be a very mature and well advanced approach - possibly the way of the future. 03-11

15. IA is all about internal controls. Internal controls are put in place to manage risk. The Board are interested in financial reporting controls which again are directed at managing risk. Also the ASX principles link audit and risk. 03-12

16. Traditionally the Audit Committee dealt with financial risk which brings in a risk perspective. Managing risk is integral to preserving over the integrity of the annual accounts in that internal controls and processes must be working properly. The Management Rep letter, which is signed by the CEO and CFO is based on systems of normal control, strong risk management and has to align with the new requirements of ASX principle no seven. 03-13

17. Both Governance activities. 03-14

18. Both are “all case, no responsibility“ functions where management is responsible and IA and RM provides a consulting, facilitation and system administration role. 03-15

19. Both are “all case, no responsibility“ functions where management is responsible and IA and RM provides a consulting, facilitation and system administration role. 03-16

20. We use the three lines of defence model, the first line being management, the second being risk management and the third is the internal and external audit. 03-17
APPENDIX TWELVE
DRAFT ABSTRACT
SENT TO S&P / ASX 200 EXECUTIVES FOR DISCUSSION AND VERIFICATION

Introduction

The corporate collapses of the late 1990’s and early 2000’s placed the concept of risk management firmly on the governance agenda. Fuelled by regulatory requirements such as the Australian Stock Exchange, Principles of Good Corporate Governance and Best Practice Recommendations (ASX Principles) boards of directors are grappling with the implementation of risk management. The recent international financial crisis, which has brought down household names such as Lehman Brothers and ABC Learning Centres, has only intensified this heat.

This research is about the governance of risk management in leading Australian companies. Using the Standard and Poor’s (S&P) / Australian Stock Exchange (ASX) 200 companies, the study looks to explain the corporate governance placed over risk management at both board committee, executive and operational levels.

The research is required because boards and executive management are struggling with governance questions around risk management and are trying to find where risk management fits into the modern organisation. The study identifies the models that Australian companies are adopting to govern risk management. The research also investigates the levels of integration between the two related disciplines of risk management and internal audit.

The research literature shows a growing integration between the internal audit and risk management functions in Canada, the United Kingdom and the United States. Combined board risk and audit committees are becoming commonplace while some companies, especially banks and derivative traders are setting up specific board risk committees (in addition to audit committees) to monitor specialised aspects of risk.

Institutional theory tells us that if internal audit and risk management are moving closer together overseas, then Australian firms will tend to adopt similar models as a method of seeking legitimacy. Given the smaller size of Australian firms, we can also predict that they might choose to integrate board committees and operational functions as an efficiency measure when faced with the escalating costs of regulation.

The study uses a mix of quantitative and qualitative methods to explore the governance of risk management in leading Australian companies. A desktop analysis of the S&P / ASX 200 explores the board committee arrangements across industry sectors. This is followed by a survey of the same companies to flesh out the reasons for governance arrangements over risk management and why different models have been chosen. Finally, interviews are conducted with a number of the S&P / ASX 200 companies to explore issues related to the governance of risk management. Such issues include the difficulties obtaining skilled directors for combined board audit and risk committees and the maintenance of internal audit independence under an integrated model.
Risk management is now arguably mandated by progressive international company regulation. To our knowledge, this research will provide the first overall study of the governance of risk management in Australia.

**Board Audit Committee**

The research found that seventy percent of S&P / ASX companies are governing risk management through the board audit committee. This could be acknowledged as the better practice. The reason for this is the natural synergy between audit and risk management. This synergy can be broken into three components:

1. The “circular flow” between audit and risk where the auditors use the risk process to design their program then find new risks to feed back into the risk process;

2. Risk management forms one leg of the “three lines of defence” model which is gaining popularity; and

3. The fact that the annual accounts are, in reality, the result of how risks have been identified and managed was seen as another link between audit and risk.

**Board Risk Committee**

The study found that twenty percent of Australian companies have a separate board risk committee (separate from the audit committee). This separate risk committee was more prominent in the financial services sector where it originated from former credit and executive lending committees. The financial services sector uses that committee to focus on credit, market, trading, operational, security, liquidity, capital, compliance, regulatory and lending mandate risks.

As suggested by the Corporate Board Member survey (2009) it is arguable whether a separate board risk committee is the better practice. The study found some issues with this model:

1. Over sixty percent of the banks indicated that they preferred the board audit committee to oversee risk;

2. Separate board risk committees tend to focus on market and trading risks rather than holistic risk management;

3. Separate board risk committees, having originated as credit or lending committees tend to be dominated by management;

4. Separate board risk committees find it difficult to capitalise on the synergy between audit and risk; and

5. Demarcation disputes often arise over committee boundaries with the audit committee.
**Skill and Timing Issues**

Generally leading Australian companies are not experiencing the problems noted in overseas literature with finding appropriately qualified directors and sufficient time at meetings. There is some evidence that the time required to manage both audit and risk matters is leading a small number of companies to consider a separate board risk committee. However, in most cases this issue is solved by having the audit committee meet more often or for a longer duration.

It appears that combined board audit and risk committees focus on audit matters around year end (April to August) and risk matters during the strategy / planning period (October to May).

**No Board Risk Committee**

The study also found that ten percent of S&P / ASX 200 companies do not have a risk committee at board level. These tend to be small companies such as mining start-ups where the full board manages risk or a committee exists at executive level.

**Executive Oversight of Risk Management**

The research found that across all S&P / ASX 200 companies, the Chief Finance Officer is still the predominant executive overseeing risk management. However, the Chief Risk Officer has taken over as the prime risk executive in the energy, telecommunication, utilities and financial services sectors.

**Integration between Audit and Risk**

Full Integration between internal audit and risk management is occurring in twenty four percent of companies where respondents stated that risk is now combined with audit. These companies see the synergy between audit and risk outweighing concerns over independence at the operational level.

For those companies who had combined risk and audit teams the majority did not see independence as an issue. For the small minority who had independence concerns, they either outsourced the auditing of risk management or established internal “Chinese walls”.

The study found that approximately thirty percent of S&P / ASX 200 companies used a partially integrated model where, although risk and audit are in separate teams, both teams report to a single executive. The remaining thirty percent have internal audit separated from risk management at the operational level, primarily due to traditional independence concerns.

Thirteen percent of companies had no risk management function and eighteen percent of the S&P / ASX 200 Australian companies have no internal audit function.
Internal Audit

The research found that eighty two percent of S&P / ASX 200 companies have some form of internal audit function. This is a large increase over the findings in earlier research. Thirty percent of companies outsource internal audit and fifty seven percent have a co-sourced arrangement. The co-sourced model usually has an in-house executive controlling the outsourced component, often through the Chief Risk Officer.

Models in Australia

Finally, bringing all of the above together and drawing on interviews with governance executives, four broad models for risk management were outlined by the S&P / ASX 200 companies. These models were discussed in terms of reporting lines, independence, maturity and whether they are forward (strategic) or backward (compliance) oriented.

Model One  Traditional Independence Model

In this structure the requirement for the internal auditor to be independent and objective dominates. The risk management team will report to a different executive to the internal audit team. The risk management function, often reporting to the CFO is a forward looking function that deals with the risks that stand in the way of achieving future objectives. The internal audit function is more of a backward looking policeman style of role. There is usually tension between management and the auditors.

Model Two  Current Merged Model

In this model risk management and internal audit both report through to the same executive. In the current merged model we are likely to see much more integration between risk and audit. With a CFO or CRO as head of strategy presiding over both risk and audit both these functions may be more forward looking functions. The risk and audit teams may work more closely together. Since the auditors mix with and contribute to management decisions (through the risk team) they are less likely to be viewed as policemen and more as a value adding part of management. Organisations that adopt such a model have the maturity to overcome the independence barriers.

Model Three  Emerging Model

In this model, the CRO has finally reached the executive team and is part of the executive decision making for the organisation. In the emerging model, many of the risk functions that traditionally reported through to the CFO have been transferred across to the CRO. Internal audit is totally integrated into the risk management culture and synergy is seen as more important than independence. The CRO will be deeply involved in strategy, ensuring all the functions that he oversees are forward looking. The risk and audit teams will work closely together and eventually may combine, losing the traditional internal audit connotation. The organisation is mature and decisions are made for the benefit of the company. The work of the risk team (including audit) is embraced by management as contributing to the greater (company) good and suggestions are welcomed rather than seen as criticism.
Model Four  No Internal Audit Model

A number of companies had no formal internal audit function but had risk management, compliance or continual improvement functions as de-facto auditors. The no internal audit model is probably a futuristic extension of the emerging model. Having functions such as risk management and continual improvement under the CRO’s guidance forces a forward looking direction. This is a very mature model where risk and audit functions exist to assist management, without some of the tensions noted in the more traditional models.
Appendix Thirteen – Example Organisational Chart

XYZ Ltd
At Board Level
- Board Risk and Audit Committee

At Management Level
- Risk and Assurance Group
  - VP Risk and Assurance
    - ERM
    - Risk & Compliance
    - Insurance
    - Group Audit Services
### Appendix Fourteen

**KEY WRITERS ON RISK MANAGEMENT**

<table>
<thead>
<tr>
<th>AUTHORS</th>
<th>Theory / Method</th>
<th>Comments</th>
</tr>
</thead>
</table>
| Subramaniam, Zhang and McManus (2009) | Signalling, Agency | **Purpose:** Agency theory used to research the factors associated with setting up a board risk committee in Australian companies.  
**Method:** Data was collected from the annual reports of the S&P / ASX 300 Australian companies, using a desk-top analysis. Logistic regression on the proportion of non-executive directors; chairman independence; board size; industry type; organisational complexity and leverage.  
**Findings:** Companies with separate board risk management committees are likely to be the larger companies, have higher financial reporting risk and lower organisational complexity. A positive relationship between board size and chairman independence with the existence of a risk committee. |
| Fraser and Henry (2007) | Contingency | **Purpose:** To investigate the ways in which companies identify risks and how internal audit and audit committees contribute to risk management.  
**Method:** Free form structured interviews with sixteen participants including listed companies and Big Four audit firms.  
**Findings:** The ongoing management of ERM by internal audit is a threat to their independence. Internal audit may lack the expertise to handle risk management, audit committees may lack the time and expertise to oversee risk management. Recommend a separate board risk committee. |
<table>
<thead>
<tr>
<th>AUTHORS</th>
<th>Theory / Method</th>
<th>Comments</th>
</tr>
</thead>
</table>
| Kleffner, Lee and McGannon (2003) | Agency          | **Purpose**: Used agency cost related factors to examine the use of ERM by Canadian companies.  
**Method**: Mail survey to members of CRIMS followed by telephone interviews.  
**Findings**: Energy companies, firms with a dedicated risk management function and reliance on Toronto Stock Exchange guidelines all led to a stronger ERM presence. |
| Liebenberg and Hoyt (2003) | Signalling, Agency | **Purpose**: To explore the determinants of the implementation of ERM in U.S. firms.  
**Method**: Used appointment of CRO as evidence of ERM, regressed against size, earnings volatility, leverage, financial opacity, ownership and location.  
**Findings**: CRO’s are concentrated in the energy and finance industries, Appointments to reduce information asymmetry. |
| Gramling and Myers (2006) | Agency          | **Purpose**: Used the maturity of ERM adoption to underpin the role of internal audit in risk management.  
**Method**: On-line survey of 7,200 IIA members through the GAIN network.  
**Findings**: Reported on the respondents view on what aspects of risk management internal auditors can become involved in and what aspects should be avoided. |
| Beasley, Clune and Hermanson (2005) | Agency          | **Purpose**: Agency theory used to identify factors associated with the implementation of ERM.  
**Method**: Logistic regression  
**Findings**: Positive correlation between ERM and the presence of a CRO, board independence, CEO and CFO support for ERM, a Big Four auditor, entity size and entities in the banking, education and insurance industries. |
| Leung, Cooper and Robertson (2004) | Agency          | **Purpose**: looked into the accountability structures, governance and management relationships of CAEs in Australian organisations  
**Method**: On-line survey to CAE’s followed by structured interviews  
**Findings**: 56% of CAE’s reported to the Audit Committee; 48% of CAE’s strongly agreed that internal audit should bring a systematic and disciplined approach to evaluating and improving the effectiveness of risk management; and 74% of CAE’s see risk management and assessment as the most important aspect of the role |
<table>
<thead>
<tr>
<th>AUTHORS</th>
<th>Theory / Method</th>
<th>Comments</th>
</tr>
</thead>
</table>
| McNamee and Selim (1998)      | None                             | **Purpose:** The research report looks at the various impacts risk management has on the internal auditing profession and the strategies now in use.  
**Method:** A rigorous literature review is followed by case study research on actual companies using different risk management models.  
**Findings:** Risk management will impact on the future structure of internal auditing. The new paradigm will see a focus on the future, less concentration on detail and more involvement in strategy. |
| Spira and Page (2002)         | Sociological perspective on risk management | **Purpose:** To explain the redefinition of internal control after the Turnbull Committee findings and the alignment between internal control and risk management.  
**Method:** Used a comprehensive literature review and a review of changes to governance practices.  
**Findings:** The paper demonstrates that developments in corporate governance reporting requirements offer opportunities for the appropriation of risk and its management by groups wishing to advance their own interests. |
| Christopher, Leung and Sarens (2009) | Agency, Institutional | **Purpose:** To review factors that might affect auditor independence in Australian companies.  
**Method:** An email based survey, sponsored by the IIA and forwarded to 206 Chief Audit Executives.  
**Findings:** Organisations operate in an environment that compromises auditor independence. |
| Goodwin-Stewart and Kent (2006) | Agency                           | **Purpose:** To examine the role of internal audit in Australian companies.  
**Method:** The study combines data from a survey of listed companies with information from corporate annual reports.  
**Findings:** Found that companies with an integrated risk management framework were more likely to adopt an internal audit function and that internal audit is complementary to other risk mechanisms. They also found that the size of the internal audit function is positively correlated to the size of the company. |
<table>
<thead>
<tr>
<th>AUTHORS</th>
<th>Theory / Method</th>
<th>Comments</th>
</tr>
</thead>
</table>
| Carey, Subramanian and Ching  | Contingency and Agency | **Purpose:** To study the use of internal auditor outsourcing in Australian companies.  
**Method:** Surveyed 1030 ASX companies and achieved a 30% response rate.  
**Findings:** Relationship between company size and outsourcing and small companies first adopting internal audit tend to outsource. |
| (2006)                        |                 |                                                                                                                                                                                                        |
| Cohen, Krishnamoorthy and     | Agency          | **Purpose:** Agency theory used to study the impact of boards and board sub-committees on the external audit process.  
**Method:** Semi-structured interviews with thirty six auditors to investigate views on corporate governance.  
**Findings:** Corporate governance mechanisms are strongly influenced by management and audit committee members often lack financial skills or sufficient power to be effective. |
| Wright (2002)                 |                 |                                                                                                                                                                                                        |
| Covaleski and Dirsmith (1988) | Institutional   | **Purpose:** To examine how key stakeholders impact on the University budgetary process;  
**Method:** Used working papers, budget submissions and interviews;  
**Findings:** High powered individuals invent and articulate expectations regarding policy and procedures. The whole process is fraught with power and self interest. |
| Rollins and Bremser (1997)    | Institutional   | **Purpose:** Investigated whether audit firm characteristics and the type of financial reporting violations are related to enforcement actions against the auditor.  
**Method:** Logistic regressions.  
**Findings:** Audit firm size and membership of the AICPA are related to disclosure violations. |
| Fogarty (1996)                | Institutional   | **Purpose:** To investigate the use of peer review programs in the self regulation of accountants.  
**Method:** Review of the peer review methodology and outcomes over time.  
**Findings:** Found a gap between the promised delivery and visible failings of the accounting profession. |
<table>
<thead>
<tr>
<th>AUTHORS</th>
<th>Theory / Method</th>
<th>Comments</th>
</tr>
</thead>
</table>
| Morris (1987)            | Signalling and Agency                          | **Purpose:** To discuss whether agency and signalling theories are competing theories or overlapping theories with many consistencies.  
**Method:** A review and comparison of the basic tenets and philosophy of both agency and signalling theory.  
**Findings:** There are consistencies between agency theory and signalling theory. Both these theoretical frameworks are based on overcoming information asymmetry and both have been used to explain, accounting choices, voluntary disclosure and the reasons for the appointment of auditors. |
| Certo (2003)             | Signalling, Institutional and Sociological Research | **Purpose:** To explain how investment promoters use board prestige as a signal for organisational legitimacy.  
**Method:** Uses signalling theory, institutional theory and sociological research to review the rationale behind IPO offerings and the boards that utilised for such offerings.  
**Findings:** Investors who purchase shares in initial public offerings (IPO's) have limited knowledge of the stewardship behind these previously private companies. This knowledge imbalance between the owner and investor creates information asymmetry. This information gap could be reduced by the company adopting a prestigious board structure using high profile individuals with high levels of social capital. This signals the quality of management to investment bankers and analysts. |
| Walker, Shenkir and Barton (2002) | Interviews and case studies | **Purpose:** Examined the role of internal auditing in the ERM process at five leading US and Canadian companies.  
**Method:** Used in-depth interviews with CAE and key executives, based on a detailed interview protocol. Case stories were prepared from interviews, verified by the companies and published.  
**Findings:** Internal audit can add significant value to ERM. Internal audit efficiency can be strengthened through involvement in ERM. Corporate governance can be strengthened by having internal audit engage in ERM. ERM is growing in importance. |
<table>
<thead>
<tr>
<th>AUTHORS</th>
<th>Theory / Method</th>
<th>Comments</th>
</tr>
</thead>
</table>
| Miccolis, Hively and Merkley  | Literature review, survey and interviews | **Purpose:** Examined the meaning of ERM, the status of ERM across industries, who is doing ERM, what results are being achieved, what tools and techniques are being used and what is the future of ERM.  
**Method:** Used a literature review, a multi industry survey and interviews with a number of leading institutions.  
**Findings:** ERM is a management tool coming into increasing vogue. The role of internal audit in ERM is likely to increase. Key challenges include, choice of conceptual model, roll out, gaining management support, what tools and metrics, use as a performance driver, link to compensation and overall communication. |
7 November 2007

Mr Steven Halliday
Group Manager Assurance
Hydro Tasmania
GPO Box 355
HOBART TASMANIA 7000

Dear Mr Halliday,

The Ethics in Human Research Committee has approved your proposal "The Governance of Risk Management in Leading Australian Companies" for a twelve month period from 7/11/2007.

The protocol number issued with respect to this project is 2007/283. Please be sure to quote this number when responding to any request made by the Committee.

Please note that the Committee requires that all consent forms and information sheets are to be printed on Charles Sturt University letterhead. Students should liaise with their Supervisor to arrange to have these documents printed.

You must notify the Committee immediately should your research differ in any way from that proposed.

You are also required to complete a Progress Report form, which can be downloaded from www.csu.edu.au/research/forms/ehre_annrep.doc, and return it on completion of your research project or by 7/11/2008 if your research has not been completed by that date.

The Committee wishes you well in your research and please do not hesitate to contact the Executive Officer on telephone (02) 6338 4628 or email ethics@csu.edu.au if you have any enquiries.

Yours sincerely

Julie Hcks
Executive Officer
Ethics in Human Research Committee
Cc: Dr Rod Dunlop Ms Kay Plummer
The Governance of Risk Management in Leading Australian Companies
Comments on Draft Survey

1. The questions are framed in a way that will provide the information set out in the research objectives.

2. The structure is logical.

3. The language used is clear and appropriate for respondents.

4. I assume that prior contact will have been made with the respondent company and the person who is to respond has been identified.

5. There will need to be an accompanying letter and/or an introductory statement.

6. Does the survey contain enough identifying demographic information for your purposes?

7. Has the instrument been approved by the Ethics Committee and what assurances will it provide about confidentiality and anonymity?

8. page 2 has two decision criteria (d).

9. On pages 2, 4, 6 and 7 you list some decision criteria or issues and ask the respondent to score them on a 5-point scale. You also make provision for the respondent to mention “other” criteria. In my view it is desirable that if they do mention any other issues or decision criteria than they should also be asked to indicate their importance using the same 5-point scale. However, there may also be value in getting a qualitative comment about any additional “issue” or “criterion”.

Tony Hocking
24 April 2008
Differentiation involved the structure of the organisation, the relationships between members over time and the member’s goal orientation (Lawrence & Lorsch 1967a, 3-4). Contingency theory proposed a number of hypotheses:

1. the greater the environmental certainty, the more formalised the structure;
2. environments exhibiting certainty will have members with more social orientation, those with uncertainty will have task oriented members;
3. members will be concerned with developing goals to cope with the environment;
4. performance at coping will be related to the level of differentiation and the degree on integration;
5. more differentiation within a sub-system means more difficulty with integration; and
6. when the environment requires both a high degree of differentiation and a high degree of integration, people will develop integrative devices.

Integration is defined by Lawrence and Lorsch as the quality of the collaboration that exists between departments to ensure unity of effort within the demands of the environment. Integration involves conflict resolution, arbitration and adjudication.

Lawrence and Lorsch (1967) used case studies to investigate the organisational structures of six plastic manufacturers, all operating in different environments. They found that each organisation set up different departments to address differing environmental characteristics. They also found that as more sub-units and departments were added, the costs of coordination increased. The optimum, it was proposed is a balance between establishing new structures to align with the environment, while integrating these structures into collective action.

The work of Lawrence and Lorsch has been extended to take in other aspects of organisational behaviour:
1. The Lorsch and Allen (1973) extension brought cognitive limitations and economic risk influences into the equation. The impact of homogeneity versus heterogeneity, or diversity of the environment is discussed; and

2. The Lawrence and Dyer (1983) extension added a number of factors that are influenced by an uncertain environment: resource availability, information complexity, the constant need to readapt and, the need for new specialists takes this extension into human resource management;
APPENDIX EIGHTEEN

THE DIFFICULTY IMPLEMENTING ENTERPRISE RISK MANAGEMENT (ERM)

The literature revealed a number of elements that a good ERM system should encompass, but equally outlined the practical and behavioural reasons why such elements are difficult to achieve. Lam (2003, p. 51) states that a successful ERM program can be broken down into a number of areas “each of these components must be developed and linked to work as an integrated whole”.

1 The Absence of Silos

ERM should span across the business without the existence of “silos” (Jorion, 2001). A siloed structure is one where departments, business units or even subsidiaries act independently within the organisation, often creating their own rules and operating in a non-collaborative manner.

The literature indicated that it is difficult to obtain buy-in from all areas in a siloed organisation and embed the ERM process into the culture. Risk management to a public relations person means something completely different to a technical project engineer. Horlick-Jones, Rosenhead, Georgiou, Ravetz and Lofstedte (2001) confirm the existence of such a drawback “not the least because corporate or inter-organisational stakeholders often have very different perceptions of the task at hand”. The 2004 PricewaterhouseCoopers annual global survey of CEO’s suggested one of the key barriers to effective ERM is the difficulty in bringing together risk management silos across the organisation. Knight (2000, p. 1) saw similar problems with the initial adoption of the AS 4360 risk standard in Australia, “it challenges strongly held beliefs, particularly of safety and/or insurance practitioners”.

2 A Strategic Focus

Sharman (2002, p. 26) maintained that “risk management strategy should be aligned with organisational strategy, the vision, mission, objectives and initiatives for growth and development. In doing so ERM remained relevant in the context of the future of the organisation, not just its current position”. The problem being experienced is that existing CEOs and the existing management team may not let risk managers into the strategy process. Robinson (2006) states that:

the fact is that most companies have a CEO and a few close people deciding the company’s future. They are risk takers and didn’t get where they are by worrying about what might go wrong. Commercial good sense dictates that they should never surrender the strategic decision process and neither will they admit to this.
3 A Portfolio Approach

Harry Markowitz introduced the concept of the portfolio approach in 1952. Using covariance, it can be shown that adding more risks to a portfolio can in some cases lower the overall probability of risk.

Tillinghast-Towers Perrin (2000) presented an example of a firm that has calculated probability distributions for fire risk, financial risk, union strike risk and entry of a new competitor risk. Using specialised software these distributions were then merged to create a single distribution which highlights where risks offset one another or reinforce one another.

However, the literature outlines a downside. Warren (2002, p. 32) argues that “such assessments cannot be easily aggregated with other loss probability distributions across the organisation. The credibility of the results may be questioned by decision makers because the method of calculation is not clear and assumptions are disputed”. In short, the software for such calculations is complex and the maths confuse everyday managers.

4 The Use of Blended Products

Another theoretical attribute of a sound ERM system is the use of blended products. The blending of insurance and financial products can produce some special products that meet integrated risks.

One early example of such an approach, a bringing together of insurance and financial risks in an integrated approach was Honeywell (Dickinson 2001). Honeywell took out a multi-year contract that combined derivatives to hedge foreign currency movements with an insurance product that covered property and liability risks.

Harrington, Niehaus, and Risko (2002) researched a case study on United Grain Growers, a Winnipeg, Manitoba based agricultural company. Through its insurer, Willis Ltd, they constructed an instrument which was essentially a put option on grain volume. Integrated with property and liability coverage the derivative pays out if industry grain volume in any one year is lower than the previous five year industry average.

However, the costs of these types of products are too expensive to make them commercially viable. Until such products gain economies of scale, they will be of limited use. Discussions with officers of Aon Insurance Pty Ltd revealed that the market for these products is highly illiquid and they are very expensive.
APPENDIX NINETEEN

SURVEY DESIGN PRINCIPLES (based on Dillman 2007)

Dillman’s (2007, p. 50 – 77) principles of survey question design:

1. chose simple over complex words;
2. chose as few words as possible to pose a question;
3. use complete sentences to ask questions;
4. avoid vague quantifiers when more precise estimates can be obtained;
5. develop response categories that are mutually exclusive;
6. avoid double barrelled questions;
7. soften the impact of potentially objectionable questions; and
8. avoid asking respondents to make unnecessary calculations.

Dillman (2007, p. 79 – 148) suggestions for survey format design:

1. A booklet style of design improves response rates, as does printing on only one side of each page (Dillman & Allen 1995). The survey was designed as a nine page booklet, printed on one page and stapled in the upper left hand corner, see Appendix Three;
2. Designing the front cover should be seen as an “opportunity to motivate the respondents”. Careful cover design can improve response rates (Nederhof, 1988 and Grembowski, 1985);
3. To achieve higher response rates, the first question should apply to everyone, be easy to answer, be short and should be interesting;
4. The order of the questions should be logical, and particular care should be taken with “skip” questions that do not apply to certain respondents;
5. Place instructions exactly where the information is needed, ask one question at a time, increased font size to attract attention and use shading and space to establish groupings. Use the largest brightest symbols to identify the starting point on each page. Use dark print for questions and light print for answer choices;
6. Answer categories should be listed vertically and answer spaces should be placed consistently to either the left or right of category labels;
7. Create visual navigation guides to help respondents follow a navigational pathway. The “Please Start Here” on page one of the survey, the three section format and having the questions in bold are all examples of that technique; and

8. Avoid specificity that exceeds the respondents potential for having an accurate ready-made answer. This issue was highlighted in the design of question twelve, where the degree of audit outsourcing or co-sourcing was requested. There could have been more alternatives, which would have only promoted definitional disputes.
## APPENDIX TWENTY

### Findings: Relationship to literature, theory and practice.

<table>
<thead>
<tr>
<th>Finding</th>
<th>Relationship to Literature</th>
<th>Theory</th>
<th>Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>73% of S&amp;P/ASX 200 have board audit committee oversight of risk management</td>
<td>Supports KPMG (2005) and Subramaniam (2009)</td>
<td>Mimetic Isomorphism.</td>
<td>If preferred model and better practice then will guide companies setting up or changing models.</td>
</tr>
<tr>
<td>17% of S&amp;P/ASX 200 have separate board risk committee</td>
<td>Unable to locate any specific prior research. ERM – second order issue</td>
<td>Signaling theory is partly responsible. GICS 40 – contingency &amp; signaling GICS 25 - signalling</td>
<td>Number of problems: 1. over 50% banks still prefer audit committee; 2. Too management heavy; 3. Unable to leverage synergy; 4. turf wars; 5. focus on financial</td>
</tr>
<tr>
<td>Synergy is main reason for having board audit committee oversight of risk management</td>
<td>Extends Subramanian (2009) by finding the reasons why companies prefer the board audit committee to oversee risk.</td>
<td>KM - synergies</td>
<td>Important for practice, reinforces that board audit committee model is preferred practice.</td>
</tr>
<tr>
<td>10% have no board risk committee.</td>
<td>Unable to locate any specific prior research</td>
<td>Smaller companies including mining start-ups</td>
<td>Can legally run risk management from full board or management committee.</td>
</tr>
<tr>
<td>Skill &amp; Timing S&amp;P/ASX 200 companies do not have these issues.</td>
<td>Contradicts Fraser and Henry (2007), Zaman (2001) and Spira and Page (2002).</td>
<td>Nothing applicable - practical</td>
<td>Found a practical way to overcome timing issues: meetings on risk during strategy time, on audit during annual accounting time.</td>
</tr>
<tr>
<td>Finding</td>
<td>Relationship to Literature</td>
<td>Theory</td>
<td>Practice</td>
</tr>
<tr>
<td>---------</td>
<td>---------------------------</td>
<td>--------</td>
<td>----------</td>
</tr>
<tr>
<td>Implementation of ERM is well developed in Australia</td>
<td>Extended Beasley (2005) and Gramling and Myers (2006) but showing implementation maturity for Australian context Kleffner Colquitt Beasley - size</td>
<td>Nothing applicable - practical</td>
<td>For practice means that ERM cannot be ignored. Some evidence of Risk Committee set up to oversee ERM</td>
</tr>
<tr>
<td>CRO is lead executive in financial, energy, IT and telecommunications</td>
<td>Supports Deloitte (2004) Liebenberg / Kleffner</td>
<td>Probably due to skill requirement to handle derivatives.</td>
<td>CRO is on the rise. Also if risk management includes complex derivatives, probably need CRO</td>
</tr>
<tr>
<td>Integration between Internal audit and risk management is happening</td>
<td>Supports Leung (2004), Goodwin-Stewart (2006) and Spira and Page (2003) and PWC (2007)</td>
<td>KM - synergies</td>
<td>Integration is OK. Benefits from synergy might outweigh independence concerns</td>
</tr>
<tr>
<td>Strict separation in 25% of companies</td>
<td>Aligns with IIA professional standards</td>
<td>Independence, but no KM or synergies</td>
<td>Traditional independence model is alive and well.</td>
</tr>
<tr>
<td>Integrated units use outsourcing, and Chinese walls and reporting lines to maintain independence</td>
<td>Aligns with Spira and Page (2003)</td>
<td>Nothing applicable practical</td>
<td>Can overcome independence problems with outsourcing, Chinese walls and reporting lines</td>
</tr>
<tr>
<td>82% of S&amp;P/ASX 200 have internal audit</td>
<td>Much higher percentage than previous studies, but different populations.</td>
<td></td>
<td>Important to note that leading companies have internal audit, but can be de-facto department.</td>
</tr>
<tr>
<td>18% of S&amp;P/ASX 200 have no internal audit</td>
<td>Unable to locate any specific prior research</td>
<td>Agency theory – smaller companies.</td>
<td>Smaller companies have no internal audit or de-facto arrangements.</td>
</tr>
</tbody>
</table>
Appendix Twenty One

Rationale for each Survey Question

Survey Question One

Question one was a demographic question on revenue. Revenue is used as an independent variable and to triangulate with the desk-top analysis, where revenues were recorded. This question was an easy introductory question aimed at gaining the respondent’s confidence and adopts Dillman’s simplicity principle. Also, revenue can be determined without the complex calculations that Dillman advises against.

Survey Question Two

For question two a Likert scale on the maturity of ERM was developed. The categories adopted are similar to those used by Beasley et al (2005) and Gramling and Myers (2006). ERM was used as an independent variable that might correlate with aspects of the risk structures adopted. Many of the writers cited in Chapter Two suggest that risk management structures may be set up to oversee the implementation of ERM. The Likert scales were designed using Dillman’s suggestion that categories should be mutually exclusive.

Survey Question Three

Question three went to the heart of this research and asked about the board audit and risk committee structure adopted. This was a primary question for the research and triangulated with the desk-top analysis. The alternative categories were developed from the desk-top analysis. The author used the KPMG (2005) and Subramaniam (2009) findings as a reconciliation check for the results from this survey. This question was originally “double barreled”, but later revised in line with Dillman’s principles.

Survey Question Four

Question four was a “skip” question where the reasons for choosing a combined board audit and risk committee structure were requested. Five Likert categories that cover possible reasons were developed. Qualitative interviews with Tasmanian risk executives and discussions with two Big Four partners contributed to the development of these categories. Using Dillman’s recommendation, the question was developed with as few words as possible.
**Survey Question Five**

Question five was aimed at determining the extent of problems with finding directors with sufficient skills and having sufficient time for audit committee meetings. The question was based on outcomes from the work by Fraser & Henry (2007) and Spira and Page (2002). These researchers outlined the problems experienced with adding risk management to the audit committee mix.

**Survey Question Six**

Question six developed a Likert scale aimed at determining the reason for setting up a separate board risk committee. The six alternatives in the Likert scale were developed from interviews with Tasmanian auditors, Tasmanian risk managers and with input from two Big Four partners.

**Survey Question Seven**

The risk management arrangement at the executive level was the objective of question seven. Drawing heavily on the work of Kleffner et al (2003) and Liebenberg and Hoyt (2003), the roles of the CFO, CRO, CAE and CEO are included in the options. Alternative or unique options were allowed for in the comments section of the survey. Again, adopting the Dillman approach, complete sentences were used to ask questions.

**Survey Question Eight**

Question eight was aimed at discovering the level of integration between internal audit and risk management at the functional or operational level. In line with Dillman’s principles, the question is kept very simple and short, avoiding difficult definitional issues and vague quantifiers.

**Survey Question Nine**

This was also a “skip” question, to be addressed by companies who have internal audit separated from risk management. A Likert scale was developed to determine why risk management is separated from internal audit. The six alternative Likert categories were developed from interviews with Tasmanian auditors, Tasmanian risk managers and from input from two Big Four partners.
Survey Question Ten
As an alternative to question nine, question ten developed a Likert scale to help determine why internal audit and risk management are combined. The five alternative Likert choices were developed from interviews with Tasmanian auditors, Tasmanian risk managers and with input from two Big Four partners.

Survey Question Eleven
Question eleven was aimed at finding out how combined audit and risk groups overcome the independence issue cited by the IIA as a barrier. Pilot interviews with Tasmanian risk managers helped establish the alternatives.

Survey Question Twelve
Question twelve established the degree of outsourcing and co-sourcing of internal audit. This question was included as an independent variable, based on the premise that companies with the outsourced model may have a different risk management structure to those with an in-house audit team.
BIBLIOGRAPHY


Australian Compliance Institute, (undated). *The 2 minute guide to compliance, ethics, governance and risk*. Downloaded from the Australian Compliance Institute website, includes comments by Mike Lotzof, the CEO of ACI.


Ernst & Young. (2007). *At the helm: insights into risk management strategy*. Produced by Ernst & Young, August 2007.


Institute of Internal Auditors, (2009). *International professional practices framework (IPPF)*. Published by the IIA Research Foundation.


The Institute of Internal Auditors Research Foundation. (2005). *ERM a status report*. Published by the IIA Research Foundation.

The Institute of Internal Auditors Research Foundation. (2006). *A global summary of the common body of knowledge*. Published by the IIA Research Foundation.


KPMG, (2005). *Strategic risk management survey*. Published by KPMG.


Protiviti, & The Institute of Internal Auditors, (2009). *Achieving high performance in internal audit*. Published by Protiviti, Melbourne, Australia.


The Institute of Internal Auditors – UK and Ireland, 2004, *The role of internal audit in enterprise wide risk management*.

The Institute of Internal Auditors (IIA), 2006, *International standards for the professional practice of Internal Auditing*, Published by IIA, Altamonte Springs, Florida USA.

The Institute of Internal Auditors (IIA), 2009, *International professional practices framework (IPPF)*, Published by IIA, Altamonte Springs, Florida USA.


